ICLG

The International Comparative Legal Guide to:

Anti-Money Laundering 2019

2nd Edition

A practical cross-border insight into anti-money laundering law

Published by Global Legal Group, with contributions from:

Allen & Gledhill LLP
Allen & Gledhill (Myanmar) Co., Ltd.
Allen & Overy LLP
AlShamsi Lawyers & Legal Consultants
Anagnostopoulos
Blake, Cassels & Graydon LLP
BONIFASSI Avocats
Castillo Laman Tan Pantaleon & San Jose
City Legal
Debevoise & Plimpton LLP
DQ Advocates Limited
Enache Pirtea & Associates S.p.a.r.l.
Gibson, Dunn & Crutcher LLP
Herbert Smith Freehills Germany LLP
JahaeRaymakers
JMiles & Co.
Joyce Roysen Advogados
Kellerhals Carrard
King & Wood Mallesons
L&L Partners Law Offices
Linklaters LLP
Marxer & Partner Attorneys at Law
McCann FitzGerald
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Nakasaki Law Firm
Nyman Gibson Miralis
Rahmat Lim & Partners
Rato, Ling, Lei & Cortés – Advogados
Rustam Kurmaev and Partners
SMM Legal Maciak Mataczyński Adwokaci Sp.k.
Vodanovic Legal
Wolf Theiss Rechtsanwälte GmbH & Co KG

glg
global legal group

global legal group

Contributing Editors
Joel M. Cohen and Stephanie Brooker, Gibson, Dunn & Crutcher LLP

Publisher
Rory Smith

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Senior Editors
Caroline Collingwood
Rachel Williams

Sub Editor
Hollie Parker

Group Consulting Editor
Alan Falach

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
May 2019

ISBN 978-1-912509-67-6
ISSN 2515-4192

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

PREFACE

We hope that you will find this second edition of *The International Comparative Legal Guide to: Anti-Money Laundering* useful and informative.

Money laundering is a persistent and very complex issue. Money laundering has been said to be the lifeblood of all financial crime, including public corruption and the financing of terrorism. Over the last 30 years, governments around the world have come to recognise the importance of strengthening enforcement and harmonising their approaches to ensure that money launderers do not take advantage of weaknesses in the anti-money laundering (AML) controls. Governments have criminalised money laundering and imposed regulatory requirements on financial institutions and other businesses to prevent and detect money laundering. The requirements are continually being refined and interpreted by government authorities. Because of the often international nature of the money laundering process, there are many cross-border issues. Financial institutions and other businesses that fail to comply with legal requirements and evolve their controls to address laundering risk can be subject to significant legal liability and reputational damage.

Gibson, Dunn & Crutcher LLP is pleased to join a group of distinguished colleagues to present several articles we hope you will find of interest on AML topics. This guide also has included chapters written by select law firms in 31 countries discussing the local AML legal and regulatory/administrative requirements and enforcement requirements. Gibson Dunn is pleased to present the chapter on the United States AML regime.

As with all ICLG guides, this guide is organised to help the reader understand the AML landscape globally and in specific countries. ICLG, the editors, and the contributors intend this guide to be a reliable first source when approaching AML requirements and considerations. We encourage you to reach out to the contributors if we can be of further assistance.

Stephanie Brooker & Joel M. Cohen

Gibson, Dunn & Crutcher LLP

To Disclose or Not to Disclose: Analyzing the Consequences of Voluntary Self-Disclosure for Financial Institutions

Stephanie Brooker

M. Kendall Day

Gibson, Dunn & Crutcher LLP

Introduction

In recent years, the benefits and drawbacks of voluntarily self-disclosing allegations of corporate misconduct to the U.S. Department of Justice ("DOJ" or the "Department") have been a topic of frequent discussion among corporate executives, in-house counsel, and white-collar practitioners. This chapter examines whether and to what extent a financial institution can expect a benefit from DOJ for making a voluntary self-disclosure ("VSD"), particularly in the context of money laundering or Bank Secrecy Act violations.

Although the public discourse regarding VSDs tends to suggest that there are significant benefits to be gained, a closer examination of the issue, specifically with respect to financial institutions, shows that the benefits a company may receive for making a VSD, if any, are neither easy to anticipate nor to quantify. A full consideration of whether to make a VSD to DOJ should include a host of factors beyond the quantifiable monetary benefit, including: (1) the likelihood of independent discovery of the alleged misconduct by law enforcement; (2) the severity, duration, and evidentiary support for a potential violation; and (3) the expectations of prudential regulators and any associated licensing or regulatory consequences, as well as other factors.

VSD decisions arise in many contexts, including in matters involving the Foreign Corrupt Practices Act ("FCPA"), sanctions enforcement, and the Bank Secrecy Act ("BSA"). In certain situations, the benefits of voluntary self-disclosure prior to a criminal enforcement action can be substantial. Prosecutors have at times responded to a VSD by reducing charges and penalties, offering deferred prosecution and non-prosecution agreements, and entering into more favorable consent decrees and settlements. However, as the second-highest official at DOJ stated in recent remarks, enforcement policies meant to encourage corporate disclosures "do not provide a guarantee" that disclosures will yield a favorable result in all cases.[1] The outcome of a prosecution following a VSD is situation-specific, and, as such, the process should not be entered into without careful consideration of the costs and benefits.

In the context of the Bank Secrecy Act and anti-money laundering regulation ("BSA/AML"), VSDs present an uncertain set of trade-offs. The BSA and its implementing regulations already require most U.S. financial institutions subject to the requirements of the BSA[2] to file suspicious activity reports ("SARs") with the U.S. government when the institution knows, suspects or has reason to suspect that a transaction by, through or to it involves money laundering, BSA violations or other illegal activity.[3] DOJ guidance encourages VSDs, and at least one recent BSA/AML non-prosecution agreement ("NPA") entered with the Department has listed self-disclosure as a consideration in determining the resolution amount.[4] Over the past three years, however, no BSA/AML criminal resolution has explicitly given an institution credit for voluntarily disclosing potential misconduct. During this same period, DOJ began messaging an expanded focus on VSDs in the context of FCPA violations, announced the FCPA Pilot Project, and ultimately codified the potential benefits of a VSD for FCPA violations in its manual for federal prosecutors.

This article addresses some of the considerations that financial institutions should weigh when deciding whether to voluntarily self-disclose potential BSA/AML violations to criminal enforcement authorities. In discussing these considerations, we review guidance provided by DOJ and the regulatory enforcement agencies, and analyze recent BSA/AML criminal resolutions, as well as FCPA violations involving similar defendants.

Uncertain Guidance from the Department of Justice

DOJ guidance documents describe the Department's general approach to VSDs, but, until recently, many questions specifically related to self-disclosures by financial institutions were left unanswered. The Department's high-level approach to voluntary self-disclosure is described in the Justice Manual ("JM"), formerly known as the United States Attorneys' Manual ("USAM"). The JM notes that "[c]ooperation is a mitigating factor" that can allow a corporation to avoid particularly harsh penalties and gives prosecutors the discretion to "consider a corporation's timely and voluntary disclosure" in deciding whether and how to pursue a corporate prosecution.[5]

In the FCPA context, the JM provides that a self-disclosure is "voluntary", and therefore potentially eligible for cooperation credit, if: (1) the company discloses the relevant evidence of misconduct prior to an imminent threat of disclosure or government investigation; (2) the company reports the conduct to DOJ and relevant regulatory agencies "within a reasonably prompt time after becoming aware of the offense"; and (3) the company discloses all relevant facts known to it, including all relevant facts about the individual wrongdoers involved.[6]

DOJ has not yet offered specific instruction, however, on how prosecutors should treat voluntary self-disclosure in the BSA/AML context and no formal self-disclosure program currently exists in the money laundering context. Indeed, the only guidance document to mention VSDs and financial institutions – issued by DOJ's National

Security Division in 2016[7] – specifically *exempted* financial institutions from VSD benefits offered to other corporate actors in the sanctions context, citing the "unique reporting obligations" imposed on financial institutions by their regulators.[8]

Despite this lack of guidance, the recent adoption of DOJ's FCPA Corporate Enforcement Policy may be indicative of how prosecutors might regard VSDs by financial institutions going forward. Enacted in the fall of 2017, the Corporate Enforcement Policy arose from DOJ's 2016 FCPA Pilot Program, which was created to provide improved guidance and certainty to companies facing DOJ enforcement actions, while incentivizing self-disclosure, cooperation, and remediation.[9] One year later, based on the success of the program, many of its aspects were codified in the USAM (now the JM).[10] Specifically, the new policy creates a presumption that entities that voluntarily disclose potential misconduct and fully cooperate with any subsequent government investigation will receive a declination, absent aggravating circumstances.[11]

Although this policy was adopted specifically in the FCPA context, DOJ's recent enforcement activity suggests the policy may be applied in other contexts, including to financial institutions. In March 2018, after an investigation by DOJ's Securities and Financial Fraud Unit, the Department publicly announced that it had opted not to prosecute a financial institution in connection with the bank's alleged front-running of certain foreign exchange transactions,[12] in part because the company had made a "timely, voluntary self-disclosure" of the alleged misconduct.[13] Principal Deputy Assistant Attorney General John Cronan, in subsequent remarks at an American Bar Association white-collar conference in which he explained DOJ's declination rationale, noted that "[w]hen a company discovers misconduct, quickly raises its hand and tells us about it, that says something.... [i]t shows the company is taking misconduct seriously...and we are rewarding those good decisions".[14] During the same speech, Cronan formally announced that the Corporate Enforcement Policy would serve as nonbinding guidance for corporate investigations beyond the FCPA context.[15]

Other Agency Guidance

Guidance issued by other enforcement agencies similarly may offer clues as to how financial institutions can utilize VSDs to more successfully navigate a criminal enforcement action.

In the context of export and import control, companies that self-disclose to the U.S. Treasury Department's Office of Foreign Asset Control ("OFAC") can benefit in two primary ways. First, OFAC may be less likely to initiate an enforcement proceeding following a VSD, as OFAC considers a party's decision to cooperate when determining whether to initiate a civil enforcement proceeding.[16] Second, if OFAC decides it is appropriate to bring an enforcement action, companies that self-disclose receive a 50 percent reduction in the base penalty they face.[17]

Other agencies tasked with overseeing the enforcement of financial regulations also have issued guidance encouraging voluntary disclosures. Although the Financial Crimes Enforcement Network ("FinCEN") has not provided guidance on how it credits voluntary disclosures,[18] guidance issued by the Federal Financial Institutions Examination Council ("FFIEC"), consisting of the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve, the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision ("OTS"), and the National Credit Union Administration ("NCUA"), has made clear that "voluntary disclosure of the violation" is among the factors the agencies will consider in determining the amount and appropriateness of a civil money penalty to be assessed against a financial institution in connection with various types of violations.[19]

In 2016, the OCC published a revised Policies and Procedures Manual to "enhance the consistency" of its enforcement decisions, including by ensuring the FFIEC factors and other relevant considerations are taken into account in its enforcement decisions.[20] That guidance includes a matrix with several factors, one of which is "concealment".[21] In the event that a financial institution self-discloses, they are not penalized for concealment. Thus, while not directly reducing potential financial exposure, a VSD ensures that a financial institution is not further penalized for the potential violation.

It is also worth noting that, unlike DOJ, these financial regulators do not appear to draw distinctions regarding the type of offense at issue (i.e., FCPA, BSA/AML, sanctions, etc.). However, financial institutions considering not disclosing potential misconduct must be mindful of whether the nature of the potential misconduct at issue goes to the financial institution's safety and soundness, adequacy of capital, or other issues of interest to prudential regulators such as the Federal Reserve, OCC, and FDIC. To the extent such prudential concerns are implicated, a financial institution may be required to disclose the underlying evidence of misconduct and may face penalties for failing to do so.

The Securities and Exchange Commission ("SEC") also has indicated that it will consider VSDs as a factor in its enforcement actions under the federal securities laws. In a 2001 report (the "Seaboard Report"), the SEC confirmed that, as part of its evaluation of proper enforcement actions, it would consider whether "the company voluntarily disclose[d] information [its] staff did not directly request and otherwise might not have uncovered".[22] The SEC noted that credit for self-reporting and other forms of self-policing could include "the extraordinary step of taking no enforcement action to bringing reduced charges, seeking lighter sanctions, or including mitigating language in documents...use[d] to announce and resolve enforcement actions".[23] In 2010, the SEC formalized its cooperation program, identifying self-policing, self-reporting, remediation, and cooperation as the primary factors it would consider in determining the appropriate disposition of an enforcement action.[24] In 2015, the former Director of the SEC's Division of Enforcement reaffirmed the importance of self-reporting to the SEC's enforcement decisions, stating that previous cases "should send the message loud and clear that the SEC will reward self-reporting and cooperation with significant benefits".[25]

Finally, like its federal counterparts, the New York Department of Financial Services ("NYDFS") has previously signaled, at least in the context of export and import sanctions, that "[i]t is vital that companies continue to self-report violations",[26] and warned that "those that do not [self-report] run the risk of even more severe consequences".[27] The NYDFS has not directly spoken to money laundering enforcement, but financial institutions considering disclosures to New York state authorities should keep this statement in mind. As with federal banking regulators, to the extent DFS prudential concerns are implicated, a financial institution may be required to disclose the underlying evidence of misconduct and face penalties for failing to do so.

Recent BSA/AML and FCPA Resolutions

Even against this backdrop, over the last few years, voluntary self-disclosure has not appeared to play a significant role in the resolution of criminal enforcement proceedings arising from alleged BSA/AML violations. Since 2015, DOJ, in conjunction with other enforcement agencies, has resolved BSA/AML charges against 12

financial institutions.[28] In 11 of those cases, the final documentation of the resolution – the settlement agreements and press releases accompanying the settlement documents – make no mention of voluntary self-disclosure. Even in the FCPA context, where DOJ has sought to provide greater certainty and transparency concerning the benefits of voluntary disclosure, there is a scant track record of financial institutions making VSDs in connection with FCPA resolutions. Since 2015, DOJ has announced FCPA enforcement actions with six financial institutions, none of which were credited for voluntarily self-disclosing the conduct at issue.[29]

Despite the paucity of recent examples of financial institutions receiving credit for VSDs, entities facing such enforcement actions should nonetheless consider how such a disclosure might affect the nature of a potential investigation and the ultimate disposition of an enforcement action. It is worth noting that in the only recent BSA/AML resolution with a financial institution in which voluntary self-disclosure *was* referenced – DOJ's 2017 resolution with Banamex USA – it was in the course of explaining why the financial institution did *not* receive disclosure credit.[30] Although there is no recent example of a financial institution receiving a lesser penalty as the result of a VSD, the fact that the Banamex USA resolution affirmatively explains why the defendant did *not* receive VSD credit may imply that this type of credit may be available to financial institution defendants when they *do* make adequate and timely VSDs.

Furthermore, over the same time period, financial institutions have been credited for other forms of cooperation in recent BSA/AML resolutions. For example, in 2015, the Department of Justice deferred prosecution of CommerceWest Bank officials for a BSA charge arising from their willful failure to file a SAR, in part because of the bank's "willingness to acknowledge and accept responsibility for its actions" and "extensive cooperation with [DOJ's] investigation".[31] Similarly, a 2015 NPA with Ripple Labs Inc. credited the financial institution with, among other factors, "extensive cooperation with the Government".[32] These favorable dispositions signal that the government is willing to grant mitigation credit for cooperation, even when financial institutions are not credited with making VSDs.

Other Relevant Considerations Relating to VSDs

As discussed above, the government's position regarding the value of VSDs and their effect on the ultimate resolution of a case may vary based on the agency and the legal and regulatory regime(s) involved. Given the lack of clear guidance from FinCEN about how it credits VSDs and the fact that BSA/AML resolutions tend not to explicitly reference a company's decision to disclose as a relevant consideration, the decision of whether to self-report to DOJ is a fraught one. Beyond the threshold question of whether or not to self-disclose to DOJ, financial institutions faced with potential BSA/AML liability should be mindful of a number of other considerations, always with an eye on avoiding a full-blown criminal investigation and trying to limit institutional liability to the extent possible.

- **Likelihood of Discovery:** A financial institution deciding whether to self-disclose to DOJ must contemplate the possibility that the government will be tipped off by other means, including by the prudential regulators, and will investigate the potential misconduct anyway, without the financial institution receiving credit for bringing a case to the government's attention and potentially before the financial institution has had the opportunity to develop a remediation plan. A financial institution planning to forego self-disclosure of possible misconduct will have to guard against both whistleblower disclosures and the possibility of another institution aware of the potential violation implicating it in a SAR filing.
- **Timing of Disclosure:** Even after a financial institution has decided to self-report to DOJ, it will have to think through the implications of when a disclosure is made. A financial institution could decide to promptly disclose to maximize cooperation credit, but risks reporting without developing the deeper understanding of the underlying facts that an internal investigation would provide. Additionally, a prompt disclosure to DOJ may be met with a deconfliction request, in which the government asks that the company refrain from interviewing its employees until the government has had a chance to do so, which can slow down the company's investigation and impede its ability to take prompt and decisive remedial actions, such as personnel decisions. Conversely, waiting until the investigation is completed, or at least more fully developed, presents the aforementioned risk of the government discovering the issue on its own. Financial institutions must also decide whether to wait until a remediation plan has already been set in motion to disclose or to disclose while the plan is still being developed.
- **Selective or Sequential Disclosures:** Given the number of agencies with jurisdiction over the financial industry and the overlaps between their respective spheres of authority, financial institutions contemplating self-disclosure will often have to decide how much to disclose, to which agencies, and in what order. In some cases, a financial institution potentially facing both regulatory and criminal liability may be well-advised to engage civil regulators first in the hope that, if DOJ does get involved, they will stand down and join a global resolution with other regulators rather than independently seeking more serious penalties. Indeed, DOJ prosecutors are required to consider the adequacy of noncriminal alternatives – such as civil or regulatory enforcement actions – in determining whether to initiate a criminal enforcement action.[33] For example, the BSA/AML NPA that DOJ entered with Banamex USA in May 2017 recognized that Citigroup, Banamex's parent, was already in the process of winding down Banamex USA's banking operations pursuant to a 2015 resolution with the California Department of Business Oversight and FDIC and was operating under ongoing consent orders with the Federal Reserve and OCC relating to BSA/AML compliance; consequently, DOJ sought only forfeiture rather than an additional monetary penalty.[34] Of course, any decision to selectively disclose must be balanced carefully against the practical reality that banking regulators will, in certain instances, notify DOJ of potential criminal violations whether self-disclosed or identified during the examination process. Whether that communication will occur often is influenced by factors such as the history of cooperation between the institutions or the relationships of those involved. In any event, a regulatory referral to DOJ might nullify any benefit to the financial institution from a selective or sequential disclosure.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Alexander Moss in the preparation of this chapter.

Endnotes

1. Rod Rosenstein, Deputy Att'y Gen., Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2017), https://www.justice.gov/opa/speech/

deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign.

2. Throughout this article, we use the term "financial institution" as it is defined in the Bank Secrecy Act. "Financial institution" refers to banks, credit unions, registered stock brokers or dealers, currency exchanges, insurance companies, casinos, and other financial and banking-related entities. *See* 31 U.S.C. § 5312(a)(2) (2012). These institutions should be particularly attuned to the role that voluntary disclosures can play in the disposition of a criminal enforcement action.
3. *See, e.g.*, 31 CFR § 1020.320 (FinCEN SAR requirements for banks); 12 C.F.R. § 21.11 (SAR requirements for national banks).
4. *See* Non-Prosecution Agreement with Banamex USA, U.S. Dep't of Justice (May 18, 2017), https://www.justice.gov/opa/press-release/file/967871/download (noting that "the Company did not receive voluntary self-disclosure credit because neither it nor Citigroup voluntarily and timely disclosed to the Office the conduct described in the Statement of Facts").
5. U.S. Dep't of Justice, Justice Manual § 9-28.700 (2017).
6. *Id.* § 9-47.120 (2017). DOJ applies a substantially identical definition in the sanctions context. *See* U.S. Dep't of Justice, Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations (Oct. 2, 2016), https://www.justice.gov/nsd/file/902491/download.
7. U.S. Dep't of Justice, Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations, at 4 n.7 (Oct. 2, 2016), https://www.justice.gov/nsd/file/902491/download. Gibson Dunn's 2016 Year-End Sanctions Update contains a more in-depth discussion of this DOJ guidance.
8. *Id.* at 2 n.3.
9. Press Release, U.S. Dep't of Justice, Criminal Division Launches New FCPA Pilot Program (Apr. 5, 2016), https://www.justice.gov/archives/opa/blog/criminal-division-launches-new-fcpa-pilot-program. For a more in-depth discussion of the original Pilot Program, see Gibson Dunn's 2016 Mid-Year FCPA Update, and for a detailed description of the FCPA Corporate Enforcement Policy, see our 2017 Year-End FCPA Update. For discussion regarding specific declinations under the Pilot Program, in which self-disclosure played a significant role, see our 2016 Year-End FCPA Update and 2017 Mid-Year FCPA Update.
10. Rod Rosenstein, Deputy Att'y Gen., Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign (announcing that the FCPA Corporate Enforcement Policy would be incorporated into the U.S. Attorneys' Manual); U.S. Dep't of Justice, Justice Manual § 9-47.120 (2017).
11. *Id.*
12. Jody Godoy, *DOJ Expands Leniency Beyond FCPA, Lets Barclays Off*, Law360 (Mar. 1, 2018), https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off.
13. U.S. Dep't of Justice, Letter to Alexander Willscher and Joel Green Regarding Investigation of Barclays PLC (Feb. 28, 2018), https://www.justice.gov/criminalfraud/file/1039791/download.
14. Jody Godoy, *DOJ Expands Leniency Beyond FCPA, Lets Barclays Off*, Law360 (Mar. 1, 2018), https://www.law360.com/articles/1017798/doj-expands-leniency-beyond-fcpa-lets-barclays-off.
15. *Id.*
16. 31 C.F.R. Pt. 501, app. A, § III.G.1 (2018).
17. *Id.* § V.B.1.a.iv (2018).
18. Robert B. Serino, *FinCEN's Lack of Policies and Procedures for Assessing Civil Money Penalties in Need of Reform*, Am. Bar Ass'n (July 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/07/07_serino/. It is worth noting, however, that there are certain circumstances in which FinCEN imposes a continuing duty to disclose, such as when there has been a failure to timely file a SAR (31 C.F.R. § 1020.320(b)(3)); failure to timely file a Currency Transaction Report (31 C.F.R. § 1010.306); and failure to timely register as a money-services business (31 C.F.R. § 1022.380(b)(3)). In circumstances in which a financial institution identifies that it has not complied with these regulatory requirements and files belatedly, the decision whether to self-disclose to DOJ is impacted by the fact that the late filing will often be evident to FinCEN.
19. Federal Financial Institutions Examination Council: Assessment of Civil Money Penalties, 63 FR 30226-02, 1998 WL 280287 (June 3, 1998).
20. Office of the Comptroller of the Currency, Policies and Procedures Manual, PPM 5000-7 (Rev.) (Feb. 26, 2016), https://www.occ.gov/news-issuances/bulletins/2016/ bulletin-2016-5a.pdf.
21. *Id.* at 15–17.
22. U.S. Secs. & Exch. Comm'n, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Release No. 44969 (Oct. 23, 2001), https://www.sec.gov/litigation/investreport/34-44969.htm.
23. *Id.*
24. U.S. Secs. & Exch. Comm'n, *Enforcement Cooperation Program*, https://www.sec.gov/spotlight/enforcement-cooperation-initiative.shtml (last modified Sept. 20, 2016).
25. Andrew Ceresney, Director, SEC Division of Enforcement, ACI's 32nd FCPA Conference Keynote Address (Nov. 17, 2015), https://www.sec.gov/news/speech/ceresney-fcpa-keynote-11-17-15.html.
26. Top Japanese Bank to Pay $250M to NY Regulators for Laundering $100B, Violating Sanctions, Star Tribune (June 20, 2013), http://www.startribune.com/japanese-bank-to-pay-ny-250m-in-laundering-case/212347271/.
27. *Id.*
28. Press Release, U.S. Dep't of Justice, U.S. Gold Refinery Pleads Guilty to Charge of Failure to Maintain Adequate Anti-Money Laundering Program (Mar. 16, 2018), https://www.justice.gov/usao-sdfl/pr/us-gold-refinery-pleads guilty-charge-failure-maintain-adequate-anti-money-laundering; Deferred Prosecution Agreement with U.S. Bancorp, U.S. Dep't of Justice (Feb. 12, 2018), https://www.justice.gov/usao-sdny/press-release/file/1035081/download; Plea Agreement with Rabobank, National Association, U.S. Dep't of Justice (Feb. 7, 2018), https://www.justice.gov/opa/press-release/file/1032101/download; Non-Prosecution Agreement with Banamex USA, U.S. Dep't of Justice (May 18, 2017), https://www.justice.gov/opa/press-release/file/967871/download; Press Release, U.S. Dep't of Justice, Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits $586 Million in Settlement with Justice Department and Federal Trade Commission (Jan. 19, 2017), https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million; Non-Prosecution Agreement Between CG Technology, LP and the United States Attorneys' Offices for the Eastern

District of New York and the District of Nevada, U.S. Dep't of Justice (Oct. 3, 2016), https://www.gibsondunn.com/wp-content/uploads/documents/publications/CG-Technology-dba-Cantor-Gaming-NPA.PDF; Press Release, U.S. Dep't of Justice, Normandie Casino Operator Agrees to Plead Guilty to Federal Felony Charges of Violating Anti-Money Laundering Statutes (Jan. 22, 2016), https://www.justice. gov/usao-cdca/pr/normandie-casino-operator-agrees-plead-guilty-federal-felony-charges-violating-anti; Press Release, U.S. Dep't of Justice, Hong Kong Entertainment (Overseas) Investments, Ltd, D/B/A Tinian Dynasty Hotel & Casino Enters into Agreement with the United States to Resolve Bank Secrecy Act Liability (July 23, 2015), https://www.justice.gov/usao-gu/pr/hong-kong-entertainment-overseas-investments-ltd-dba-tinian-dynasty-hotel-casino-enters;Deferred Prosecution Agreement with Bank of Mingo, U.S. Dep't of Justice (May 20, 2015), https://www.gibsondunn.com/wp-content/uploads/documents/publications/Bank-of-Mingo-NPA.pdf; Settlement Agreement with Ripple Labs Inc., U.S. Dep't of Justice (May 5, 2015), https://www.justice.gov/file/421626/download; Deferred Prosecution Agreement with Commerzbank AG, U.S. Dep't of Justice (March 12, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/12/commerzbank_deferred_prosecution_agreement_1.pdf; Deferred Prosecution Agreement with CommerceWest Bank, U.S. Dep't of Justice (March 10, 2015) https://www.justice.gov/file/348996/download.

29. Deferred Prosecution Agreement with Société Générale S.A., U.S. Dep't of Justice (June 5, 2018), https://www.justice.gov/opa/press-release/file/1068521/download; Non-Prosecution Agreement with Legg Mason, Inc., U.S. Dep't of Justice (June 4, 2018), https://www.justice.gov/opa/pressrelease/file/1068036/download; Non-Prosecution Agreement with Credit Suisse (Hong Kong) Limited, U.S. Dep't of Justice (May 24, 2018), https://www.justice.gov/opa/press-release/file/1077881/download; Deferred Prosecution Agreement with Och-Ziff Capital Management Group, LLC, U.S. Dep't of Justice (Sept. 29, 2016), https://www.justice.gov/opa/file/899306/download; Non-Prosecution Agreement with JPMorgan Securities (Asia Pacific) Limited, U.S. Dep't of Justice (Nov. 17, 2016), https://www.justice.gov/opa/press-release/file/911206/download; Non-Prosecution Agreement with Las Vegas Sands Corp., U.S. Dep't of Justice (Jan. 17, 2017), https://www.justice.gov/opa/press release/file/ 929836 /download.

30. *See* Non-Prosecution Agreement with Banamex USA, U.S. Dep't of Justice, at 2 (May 18, 2017), https://www.justice.gov/opa/press-release/file/967871/download (explaining that Banamex "did *not* receive voluntary disclosure credit because neither it nor [its parent company] Citigroup voluntarily and timely disclosed to [DOJ's Money Laundering and Asset Recover Section] the conduct described in the Statement of Facts") (emphasis added).

31. Deferred Prosecution Agreement Between United States and CommerceWest Bank, U.S. Dep't of Justice, at 2–3 (Mar. 9, 2015), https://www.justice.gov/file/348996/download.

32. Settlement Agreement Between United States and Ripple Labs Inc., U.S. Dep't of Justice (May 5, 2015), https://www.justice.gov/file/421626/download; *see also* Press Release, U.S. Dep't of Justice, Ripple Labs Inc. Resolves Criminal Investigation (May 5, 2015), https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation.

33. See Justice Manual § 9-28.1200 (recommending the analysis of civil or regulatory alternatives).

34. Non-Prosecution Agreement Between U.S. Dep't of Justice, Money Laundering and Asset Recovery Section and Banamex USA, at 2 (May 18, 2017), https://www.justice.gov/opa/press-release/file/967871/download.

Stephanie Brooker

Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W
Washington, D.C. 20036
USA

Tel: +1 202 887 3502
Email: sbrooker@gibsondunn.com
URL: www.gibsondunn.com

Stephanie L. Brooker, former Director of the Enforcement Division at the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and a former federal prosecutor, is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is Co-Chair of the Financial Institutions Practice Group and a member of White Collar Defense and Investigations Practice Group. As a prosecutor, Ms. Brooker tried 32 criminal trials, investigated a broad range of white-collar and other federal criminal matters, briefed and argued criminal appeals, and served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia. Ms. Brooker's practice focuses on internal investigations, regulatory enforcement defense, white-collar criminal defense, and compliance counseling. She handles a wide range of white-collar matters, including representing financial institutions, multi-national companies, and individuals in connection with criminal, regulatory, and civil enforcement actions involving sanctions, anti-corruption, anti-money laundering (AML)/Bank Secrecy Act (BSA), securities, tax, wire fraud, and "me-too" matters. Ms. Brooker's practice also includes BSA/AML compliance counseling and due diligence and significant criminal and civil asset forfeiture matters. Ms. Brooker was named a 2018 National Law Journal White Collar Trailblazer and a Global Investigations Review Top 100 Women in Investigations.

M. Kendall Day

Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W
Washington, D.C. 20036
USA

Tel: +1 202 955 8220
Email: kday@gibsondunn.com
URL: www.gibsondunn.com

M. Kendall Day is a partner in the White Collar Defense and Investigations and the Financial Institutions Practice Groups at Gibson Dunn. He represents multi-national companies, financial institutions, and individuals in matters involving anti-money laundering (AML)/Bank Secrecy Act (BSA), sanctions, FCPA and other anti-corruption, securities, tax, wire and mail fraud, unlicensed money transmitter, and sensitive employee issues.

Prior to joining Gibson Dunn, Mr. Day spent 15 years as a white-collar prosecutor with the Department of Justice (DOJ), rising to the highest career position in the DOJ's Criminal Division as an Acting Deputy Assistant Attorney General (DAAG). Mr. Day also previously served as Chief and Principal Deputy Chief of the Money Laundering and Asset Recovery Section. In these various leadership positions, from 2013 until 2018, Mr. Day supervised many of the country's most significant cases involving allegations of corporate and financial misconduct, and he exercised nationwide supervisory authority for all cases involving AML and financial institutions.

GIBSON DUNN

Gibson, Dunn & Crutcher LLP is a full-service global law firm, with more than 1,300 lawyers in 20 offices worldwide. In addition to 10 locations in major cities throughout the United States, we have 10 in the international financial and legal centers of Beijing, Brussels, Dubai, Frankfurt, Hong Kong, London, Munich, Paris, São Paulo and Singapore. We are recognised for excellent legal service, and our lawyers routinely represent clients in some of the most complex and high-profile matters in the world. We consistently rank among the top law firms in the world in published league tables. Our clients include most of the Fortune 100 companies and nearly half of the Fortune 500 companies.

Board Oversight of AML Risk: How Directors Can Navigate an Evolving World

Matthew Biben

Meryl Holt Silverman

Debevoise & Plimpton LLP

Introduction

In 2018, U.S. financial regulators and prosecutors imposed more than $1 billion in fines related to anti-money laundering ("AML") compliance failures.[1] A theme that emerges from these enforcement actions is the continued emphasis on the role of individual compliance officers, senior executives, and board members, including attempts to hold these individuals personally accountable.[2]

The focus on personal liability extends well beyond AML enforcement, forcing a spotlight onto the general oversight and compliance obligations of bank boards of directors. In particular, the penalties imposed on Wells Fargo by the Federal Reserve in February 2018 in connection with allegedly fraudulent sales practices demonstrate regulators' interest in and expectations with regard to board accountability, and have been characterised as "an attempt by the Fed to impress upon banks that their boards of directors should be vigorous, independent watchdogs – and if they fail, there will be consequences".[3]

Accordingly, the onus is on directors of financial institutions to ask the right questions to understand the bank's business and identify and prioritise the associated risks. It is critical to understand what is needed to effectively oversee and hold management accountable for complying with AML laws and regulations, as well as how to evaluate the bank's AML policies and programme. But the questions board members should ask extend well beyond financial and compliance risks to those associated with corporate culture, strategy, and operations.

This article outlines the duties of directors of financial institutions and offers a roadmap for board members trying to navigate the basic AML requirements and related key risk indicators, and their place in effective enterprise risk management, including management of strategic and operational risks that implicate a bank's business model and reputation. The considerations set forth herein have particular salience in the context of emerging – and potentially higher risk – sectors, such as cryptocurrency and marijuana, which may pose unique oversight and monitoring challenges.

Duties of Directors

In the United States, the framework for fiduciary duties and responsibilities of members of boards of directors emerges out of common law, with further definition imposed by state statutes and evolving case law.[4] The duties of care and loyalty are viewed as the traditional fiduciary duties owed by directors to the corporation, and directors are expected to carry out their corporate obligations in good faith.[5] Courts have interpreted these overarching duties as giving rise to an array of subsidiary duties that comprise director responsibilities, which can be broadly categorised as (1) the duty to exercise oversight – by remaining informed about the corporation, regularly reviewing financial statements, and inquiring into corporate affairs, for example – and (2) the duty to actively monitor performance against risk parameters as well as corporate strategy in light of attendant risks.[6]

The Delaware Court of Chancery set out the standard for directors' duty to oversee and actively monitor the corporation in *Caremark*, holding that corporate directors have an affirmative duty to establish, and exercise appropriate oversight over, some form of internal compliance activity.[7] Internal controls must be "rationally designed", though the level of detail of the control framework is a matter of business judgment.[8] In the event directors become aware of red flags, due to internal controls or through other means, they have a duty to take action.[9] *Caremark* sets a high standard for a director's breach of oversight obligations, noting that "only a sustained or systemic failure of the board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability".[10]

Decisions following *Caremark* flesh out the contours of directors' fiduciary obligations. In 2012, the Delaware Court of Chancery clarified that there is a distinction between inadequate or flawed efforts and a conscious disregard by directors to meet their duty to monitor and oversee the corporation.[11]

While *Caremark* sets a demanding standard, the Wells Fargo shareholder derivative litigation offers an example of allegations involving board processes and decision-making that could result in director liability.[12] Plaintiff shareholders sued, in relevant part, the directors of Wells Fargo, alleging that they "knew or consciously disregarded that Wells Fargo employees were illicitly creating millions of deposit and credit card accounts for their customers, without those customers' knowledge or consent".[13] In particular, plaintiffs alleged that directors allowed Wells Fargo to defraud customers through "cross-selling" activities.[14] The complaint stated that the directors knew about the alleged fraudulent activity because, among other things, they were aware of letters from employees voicing concerns, complaints made through the bank's ethics hotline, lawsuits related to the fraudulent sales practices, and investigations by government agencies.[15] Plaintiffs further alleged that the defendant directors failed to ensure compliance with applicable laws, facilitated the fraudulent activity through poor oversight, and caused the bank to issue false or misleading financial statements and reports.[16]

In denying Wells Fargo's motion to dismiss and holding that the allegations met *Caremark*'s standard of conscious failure of

oversight, the court repeatedly referenced allegations that the directors had personal awareness of various red flags concerning Wells Fargo's sales practices.[17] Moreover, the court emphasised the sheer number of red flags that "collectively…support[ed] an inference that a majority of the Director Defendants consciously disregarded their fiduciary duties despite knowledge regarding widespread illegal account-creation activities, and…that there is a substantial likelihood of director oversight liability".[18] This case, while an outlier,[19] emphasises the need for directors to heed repeated indicators of a certain type of misconduct, as courts may construe the absence of a clear response as a conscious disregard to meet the duty to monitor and oversee the corporation.

Taken together, *Caremark* and subsequent cases require bank board members to stay informed about matters that could affect "judgments concerning both the corporation's compliance with law and its business performance".[20] These cases suggest that directors should put in place a formal process that routinises communications between the board and management regarding risk indicators compiled in the ordinary course and more pressing matters subject to escalation. Through this process, directors should proactively solicit and review timely and accurate information, not only about the compliance framework and business performance, but also about the broader environment and industries in which the bank is operating.

Three Lines of Defence

As a threshold matter, bank directors should familiarise themselves with the three lines of defence model, a widely adopted risk management framework. The three lines of defence model is designed to help complex organisations, such as banks, define the roles and responsibilities of front-line business personnel, practice ongoing risk management, and maintain risk management activities.[21]

The first line of defence consists of frontline employees and managers whose role is to manage risks and controls on a day-to-day basis. The second line supports senior management by establishing policies and procedures and overseeing the first-line risk management process. Meanwhile, the third line is an independent assurance function performed by internal auditors who review the corporation's risk management, controls, and governance processes at a systemic level. Internal audit generally reports independently to the board or the audit committee. The role of the board is to provide a "credible challenge" to the information and views provided by management as it carries out implementation of this risk management system.[22]

A director is expected to monitor implementation of the three lines of defence framework and be comfortable that there is sufficient information sharing and coordination among the three lines to allow for effective AML compliance risk management.

BSA/AML Risk Oversight[23]

There are various ways to keep abreast of basic AML compliance programme requirements and expectations, starting with the Federal Financial Institutions Examination Council Bank Secrecy Act ("BSA")/Anti-Money Laundering Examination Manual (the "FFIEC Manual").[24] The FFIEC Manual makes clear that the "board of directors, acting through senior management, is ultimately responsible for ensuring that the bank maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the bank's BSA/AML policies, procedures, and processes".[25]

Effective board oversight is supported by establishing a presentation calendar that includes regular reporting by key members of the management team, including the designated BSA compliance officer. Management is responsible for keeping the board adequately informed about risk-taking activities, which should include routine updates on key performance measurements and risk indicators that reflect the overall health of the bank's AML compliance programme. The Office of the Comptroller of the Currency ("OCC") publishes guidance that offers specific AML-related questions for directors to consider and ask based on this data.[26]

The board also has an obligation to continuously consider whether the information it receives is sufficient information upon which to make informed decisions. Directors may conclude that the board should meet with management with greater frequency, a special session of the board is necessary to collect additional information on a particular topic, an executive session of the board is needed with or without specific members of management, or engagement with management beyond the boardroom is required. Ensuring an open channel of communication with management is important, as is the ability of key officers to speak openly with the board about AML compliance issues, particularly the resources needed to address potential programme deficiencies.

In light of key issues that have been the subject of recent AML enforcement actions, directors should make sure that regular communications with management cover the following topics in relation to the bank's AML policies and procedures.

Assessing an AML Compliance Programme

Directors should first review, on a periodic basis, the bank's AML risk assessment. This risk assessment should measure inherent risk, which is the risk that an activity would pose if no controls or other mitigating factors were in place.[27] A residual risk rating should be assigned after controls are taken into account. The assessment should be candid and self-critical, especially in describing the inherent risks of doing business in a high-risk jurisdiction or providing high-risk financial services.[28] Smaller banks may not have formal written assessments, but should still engage in and document the assessment process.

Second, directors should expect regular reporting from management regarding any uncorrected supervisory issues contained in written agreements, enforcement actions, or matters requiring attention. Although criminal law enforcement agencies may identify compliance failures in the course of their investigations, most enforcement actions are brought by regulators such as the Federal Reserve or the Federal Deposit Insurance Corporation for uncorrected deficiencies previously cited during routine exams. In overseeing and holding management accountable for fixing these problems, directors should be wary of proposed solutions involving technological upgrades that might prove to be unfeasible or will take too long to implement. Board members should request regular updates from management and tracking of important milestones to ensure that deficiencies are being addressed in a timely manner.

Third, directors should know whether the bank has any uncorrected AML deficiencies identified by outside consultants. Senior managers and compliance officers at times retain outside experts to review the firm's AML compliance programme.[29] Such reviews may be triggered by unfavourable audit or exam findings, pending enforcement actions, or management's desire to proactively find and address problems. Recent AML enforcement actions have highlighted the risks to financial institutions of failing to act on

documented AML deficiencies, or withholding these third-party reports from regulators.[30] If the BSA compliance officer is new to the firm, directors should ask this individual to check the files for reports commissioned and left behind by the former BSA compliance officer.

Finally, it is important for directors to understand which employees receive AML training and what guidance is provided with respect to suspicious activity reporting. Financial institutions must ensure that appropriate personnel are trained in applicable aspects of the BSA.[31] Directors typically receive training that is tailored to their oversight role, including approving BSA/AML policies and ensuring that management is providing sufficient BSA/AML resources. But a deeper dive into questions related to who else is receiving such training and how often employees are identifying and reporting activity should provide insight into the firm's culture of compliance and whether AML compliance is viewed as a company-wide responsibility.

Identifying and Responding to Red Flags

In addition to assessing the general health of the bank's AML compliance programme, there are various topics that are key to evaluating the organisation's capacity to identify and respond to red flags. Directors should, for instance, be aware of whether the bank collects and analyses consumer and fraud complaints, and whether there are any ongoing government investigations concerning fraud by or through the bank. It is important to engage with management to understand possible fraud occurring at or through the institution, such as internet-based scams resulting in victims sending numerous but relatively small dollar transactions through the institution. In recent years, criminal prosecutors have demonstrated interest – in the form of prosecutions and large fines – for firms failing to detect, report, and halt such transactions.[32]

Directors also should inquire into the volume of suspicious activity reports ("SARs") filed through the Financial Crimes Enforcement Network ("FinCEN"), including how these numbers stand relative to the bank's peers and agency statistics. Disclosures of specific SAR filings outside of the filing institution are prohibited, but AML compliance officers are encouraged to share this information with board members. Directors should therefore expect reporting from management on key risk indicators, including, but not limited to: changes in volume with respect to transaction alerts, which identify unusual account or customer activity that may indicate financial crimes; timeline metrics, such as the average length of time between the identification of potential suspicious activity and filing of a SAR; and data that show significant spikes, drop-offs, or other changes in the volume of SAR filings. Of particular concern is under-filing of SARs, which poses greater enforcement risk than over-filing.[33] Board members should inquire about tracking of "no-SAR" decisions – *i.e.*, when potential suspicious activity is flagged but BSA staff declines to file a SAR – to make sure management is focused on evaluating and mitigating any weaknesses in organisational decision-making and record-keeping in the event of a future regulatory inquiry.

Beyond SARs and BSA requirements, compliance with sanctions regulations administered by the Office of Foreign Assets Control ("OFAC") requires financial institutions to block accounts and other property of specified countries, entities, and individuals, or prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.[34] In some instances, a bank may fail to block or reject prohibited accounts or transactions that might, upon review by the OFAC, expose the company to significant fines. Asking what transactions the institution has failed to identify and block is a good starting point in assessing the institution's customer base and risk profile.

In view of the above, directors should take a critical eye as to whether the bank has sufficient AML resources and staff. Directors must also consider whether there are Audit staff members who are competent and knowledgeable to test the AML programme. A potentially important gauge on this point is the rate of employee attrition for these departments. All institutions, large and small, at times experience significant increases in investigative caseloads that may lead to employee attrition and the loss of important institutional knowledge, and that may require devotion of additional resources. Consequently, directors should work with management to monitor staff adequacy based on caseload and average throughput per investigator. Directors should also endeavour to find out if the bank has a backlog with respect to compliance alerts or cases in order to protect the institution from potential supervisory action.

The Intersection of AML & Enterprise Risk Management

Opportunities presented by emerging industries such as cryptocurrency and marijuana demonstrate the intersection of AML risk and sanctions considerations with enterprise risk management, which implicates the bank's overall risk appetite and compliance culture. Board oversight mechanisms should be designed to accommodate these new opportunities, but directors should be aware that choices regarding engagement with these sectors may have a significant effect on the bank's business model, capabilities, resources, and reputation. As a result, risk management requires not only clear-eyed attention to the legal and regulatory challenges, but also the operational competence and agility to capitalise on new developments.

Cryptocurrency

As evidenced by JPMorgan's announcement of JPM Coin in February 2019, banks are starting to move beyond exploration of blockchain and arguably into cryptocurrency.[35] This move follows rapid growth and increased investment in the cryptocurrency and initial coin offering markets and takes place against a backdrop of heightened regulatory scrutiny.

FinCEN has made clear since 2013 that all sellers of cryptocurrency tokens, including in the context of an initial coin offering, are money services businesses and must comply with applicable AML requirements.[36] Yet, the regulatory landscape continues to evolve as the industry develops and the various federal agencies tasked with enforcement, including the Securities and Exchange Commission, the Commodity Future Trading Commission, and the Department of Justice, engage in closer coordination. While cryptocurrencies present many of the same risks as other financial technological innovations, peer-to-peer transaction authentication and the ability to operate independently of institutional intermediaries trained in AML compliance result in a unique set of challenges, both for financial institutions and their regulators.[37]

The same features of cryptocurrency that render it innovative – its anonymity, absence of national borders, and liquidity – result in heightened AML and sanctions risks of which banks and their boards of directors should be keenly aware. In particular, counterparty anonymity may pose a challenge to key elements of the bank's AML programme, including Know Your Customer and customer identification procedures. The cryptocurrency markets are also potentially exposed to risks such as facilitation of illicit

transactions and the transfer of unlawful proceeds, unknown touchpoints with criminal enterprises, as well as terrorism financing or evasion of sanctions. There is, for instance, evidence that terrorist groups have been experimenting with cryptocurrencies since 2014, including through social media campaigns aimed at raising Bitcoin for such groups.[38] Moreover, the absence of a finely-tuned regulatory framework for the ever-changing cryptocurrency markets makes it especially difficult to detect and deter bad actors.

A board and management also may ensure that their due diligence, account transaction monitoring, and suspicious activity reporting procedures are robust and efficacious with respect to dealings in cryptocurrency. It may be that the development of tailored transaction flags and employee trainings is appropriate given the special features of crypto-businesses. A board may also decide that it is not possible to mitigate fully the risks that cryptocurrency currently presents and decline to pursue the business.

Marijuana

The burgeoning marijuana industry in the United States also presents a set of unique challenges given the current rift between federal and state drug laws. Marijuana is a Schedule I controlled substance in the United States pursuant to the Controlled Substances Act ("CSA"), which prohibits, among other conduct, the production, sale, and distribution of marijuana.[39] However, with 10 states and the District of Columbia allowing recreational use of marijuana and a majority of states allowing use of marijuana for medical purposes, financial institutions are faced with addressing the challenges of legalisation at the state level even as it remains federally illegal. Pressures along the U.S. border also abound, as Canada recently legalised recreational consumption of marijuana and Mexico is considering similar legislation.[40]

The primary risk from the perspective of a financial institution is attachment of U.S. criminal liability under a theory of aiding and abetting a violation of or conspiring to violate the CSA and/or under AML statutes, which prohibit financial transactions involving the proceeds of "specified unlawful activity". "Specified unlawful activity" covers the manufacture, importation, sale, or distribution of a controlled substance, as defined under the CSA.[41]

For liability to attach to a financial firm under either U.S. drug laws or AML provisions, there must be: (1) a nexus between the marijuana-related business activities and the United States;[42] or (2) conduct that violates Canadian or other applicable local law.[43] The nexus requirement may be satisfied where a financial institution holds deposits for a marijuana-related business or trades in the securities of an entity engaged in U.S. marijuana-related activities.

As a statutory matter, the risk of federal prosecution in connection with marijuana-related activity in or touching the United States is plausible, but authorities have to date adhered to a policy of nonenforcement with respect to legitimate marijuana activities in states where the substance is legal. Meanwhile, marijuana-related activities in Canada bear a different risk profile: where an entity conducts marijuana-related activities only in Canada, and does so in full compliance with Canadian law, the provision of financial services to such a business should not violate U.S. federal criminal laws so long as there is no indication that the marijuana is being imported from or exported into the United States.

Financial institutions that are considering banking marijuana-related businesses, therefore, must consider not only their risk appetite in light of the potential for federal criminal liability with respect to U.S.-facing marijuana activities, but also reputational risks given that most major financial institutions have been leery of engaging with the industry. Key to any engagement with the marijuana industry is the implementation of an operational framework aimed at verifying compliance with applicable Canadian and U.S. laws, monitoring for marijuana-related activities that may touch the United States, and carrying out vigilant SAR compliance.

Managing Enterprise Risks

In managing risks associated with emerging industries, directors should ensure that their bank updates its policies and procedures in a way that accounts for the (1) particular AML risks associated with those sectors, (2) operational challenge of ensuring consistent treatment of these clients across business lines, and (3) potential for rapid changes in the legal and regulatory environment. While management is responsible for implementing an AML compliance framework tailored to the inherent challenges of higher-risk industries, directors can and should play an important role in understanding the risks, charting a strategic approach, and monitoring management's adherence to that strategy and the bank's risk appetite.

Directors should be sure to engage – and provide a credible challenge to – management in periodic discussions aimed at developing a shared understanding of how much risk the bank wishes to take, which will set the risk appetite across the organisation. Further, discussions about the opportunities presented in areas such as cryptocurrency and marijuana should include a robust debate regarding the attendant risks of those activities, both legal and reputational. These conversations should allow management to elevate risks to the board in a way that facilitates directors' ability to oversee the bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may question, challenge, and at times oppose decisions made by management that might cause the bank to exceed its risk appetite or even jeopardise safety and soundness.[44]

Conclusion

In sum, the responsibilities of bank directors extend well beyond assessing and monitoring SARs and discrete financial regulatory requirements. Developments since *Caremark* suggest that directors are being held to a higher standard, and should pay particular attention not only to repeated indicators of problematic activity, but also to risks in emerging sectors with the potential to disrupt the business and create regulatory headaches. Ongoing monitoring of AML risks should translate into effective enterprise risk management, including management of strategic and operational risks that implicate a bank's business model and reputation. Done properly, this approach should protect stakeholders while helping the bank anticipate and mitigate key risks.

Endnotes

1. Matthew L. Biben *et al.*, 2018/2019 Anti-Money Laundering Review and Outlook, Debevoise In Depth (Feb. 5, 2019), https://www.debevoise.com/~/media/files/insights/publications/2019/01/20190205_2018_anti_money_laundering_review_and_outlook.pdf. For purposes of this article, we use the term "AML" to refer to Bank Secrecy Act, AML, and sanctions rules for financial institutions, as well as related state laws and regulations.
2. Enforcement actions resulting in personal liability for compliance officers have become increasingly common. *See* Press Release, U.S. Dep't of Justice, Acting Manhattan U.S. Attorney Announces Settlement Of Bank Secrecy Act Suit

Against Former Chief Compliance Officer At Moneygram For Failure To Implement And Maintain An Effective Anti-Money Laundering Program And File Timely SARS (May 4, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-settlement-bank-secrecy-act-suit-against-former; Press Release, U.S. Dep't of Justice, Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million (Feb. 7, 2018), https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

3. Emily Flitter *et al.*, *How Wells Fargo and Federal Reserve Struck Deal to Hold Bank's Board Accountable*, New York Times (Feb. 4, 2018), https://www.nytimes.com/2018/02/04/business/wells-fargo-fed-board-directors-penalties.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news/.
4. *See, e.g.*, Theodor Baums & Kenneth E. Scott, *Taking Shareholder Protection Seriously? Corporate Governance in the United States and Germany*, 53 Am. J. Comp. L. 31, 37 (2005) (explaining that the U.S. "fiduciary duty concept is derived from the common law of trusts, but has been modified in its application to the business context"); *CTS Corp. v. Dynamics Corp. of. Am.*, 481 U.S. 69, 89 (1987) ("[n]o principle of corporation law and practice is more firmly established than a State's authority to regulate domestic corporations").
5. *In re Walt Disney Co. Derivative Litig.*, 907 A.2d 693, 745 (Del. Ch. 2005), *aff'd*, 906 A.2d 27 (Del. 2006) ("The fiduciary duties owed by directors … are the duties of due care and loyalty … and the duty of a director to act in good faith").
6. *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996) (duty to oversee and monitor); *Francis v. United Jersey Bank*, 432 A.2d 814, 822 (N.J. 1981) (duty to conduct regular review of financial statements); *Barnes v. Andrews*, 298 F. 614, 615 (S.D.N.Y. 1924) (duty to inquire into corporate affairs).
7. *Caremark*, 698 A.2d at 959.
8. *Id.* at 970.
9. *Id.* at 971.
10. *Id.*
11. *Louisiana Mun. Police Employees' Ret. Sys. v. Pyott*, 46 A.3d 313, 341 (Del. Ch. 2012) ("The decision to act and the conscious decision not to act are thus equally subject to review under traditional fiduciary duty principles").
12. *In re Wells Fargo & Co. S'holder Derivative Litig.*, 282 F. Supp. 3d 1074 (N.D. Cal. 2017).
13. *Id.* at 1082.
14. *Id.*
15. *Id.* at 1082–83.
16. *Id.* at 1083.
17. *Id.* at 1107-09 (citing *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 370 (Del. 2006)).
18. *Id.* at 1088, 1107-09 (alteration in original).
19. On seemingly similar facts, a court considering shareholder derivative litigation against Citigroup held that plaintiffs failed to allege facts sufficient to meet the *Caremark* standard. *Oklahoma Firefighters Pension & Ret. Sys. v. Corbat*, No. 12151-VCG, 2017 WL 6452240 (Del. Ch. December 18, 2017).
20. *Caremark*, 698 A.2d at 970.
21. *See*, *e.g.*, KPMG LLP, *The three lines of defense* (2016), https://assets.kpmg/content/dam/kpmg/ca/pdf/2017/01/three-lines-of-defense-kpmg.pdf.
22. Off. of the Comptroller of the Currency, *Corporate and Risk Governance* (July 2016), at 42, 46–47, https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf.
23. *See* Matthew L. Biben, *So You Want to Join a Bank Board? Ask About AML Risk Oversight*, New York Law Journal (November 15, 2018), https://www.law.com/newyorklawjournal/2018/11/15/so-you-want-to-join-a-bank-board-ask-about-aml-risk-oversight/.
24. Fed. Fin. Insts. Examination Council, *BSA/AML Compliance Program – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_007.htm (last modified July 26, 2017).
25. *Id.*
26. Off. of the Comptroller of the Currency, *Director's Toolkit*, https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/directors-toolkit.html (accessed Feb. 18, 2019).
27. The Wolfsberg Group, *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* § 7, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf (last modified September 4, 2015).
28. *Id.*
29. Fin. Crimes Enf't Network, *Frequently Asked Questions: Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs* (September 22, 2006), https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-conducting-independent-reviews.
30. *See* Laura Akahoshi, Off. of the Comptroller of the Currency Notice # N18-002 (notice of charges for order of prohibition and assessment of a civil money penalty April 16, 2018), www.occ.gov/static/enforcement-actions/eaN18-002.pdf; Jesse Hamilton & Tom Schoenberg, *CEO of Bank That Hid Drug Cash Faces U.S. Criminal Probe*, Bloomberg (May 10, 2018).
31. Fed. Fin. Insts. Examination Council, *BSA/AML Compliance Program – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_007.htm (last modified July 26, 2017).
32. Fed. Trade Comm'n, *Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department* (January 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles; Fin. Indus. Regulatory Auth., *Finra Fines LPL $2.75 Million for Complaint-Reporting and AML Program Failures* (October 30, 2018), https://www.finra.org/newsroom/2018/finra-fines-lpl-2-point-75-million-for-complaint-reporting-and-aml-program-failures.
33. *See* Aegis Capital Corp., Exchange Act Release No. 82956 (cease and desist order Mar. 28, 2018), https://www.sec.gov/litigation/admin/2018/34-82956.pdf; Sec. Exch. Comm'n, *SEC Charges Brokerage Firms and AML Officer with Anti-Money Laundering Violations* (May 16, 2018), https://www.sec.gov/news/press-release/2018-87.
34. Fed. Fin. Insts. Examination Council, *Office of Foreign Assets Control – Overview*, Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_037.htm (last modified July 26, 2017).
35. Michael del Castillo, *Jamie Dimon's Cryptocurrency Master Plan Swipes At Swift*, Forbes (Feb. 14, 2019),

https://www.forbes.com/sites/michaeldelcastillo/2019/02/14/jaime-dimon-finally-shows-jp-morgans-cryptocurrency-hand/#37f1a4b2e7ed. It is important to note, however, that JPM Coin has been described by many as being more akin to an in-house electronic payment system than a cryptocurrency. Unlike cryptocurrency, which is open, permission-less, and available to the public for download, JPM Coin will run on a private blockchain and operate within a closed, permissioned network. *See* Aaron Hankin, *JPM Coin is not a cryptocurrency, says crypto advocacy group*, MarketWatch (Feb. 15, 2019), https://www.marketwatch.com/story/jpm-coin-is-not-a-cryptocurrency-says-crypto-advocacy-group-2019-02-14.

36. *FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

37. FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, at 9–10 (June 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

38. Zachary K. Goldman *et al.*, *Terrorist Use of Virtual Currencies*, Center for a New American Security (May 2017), lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

39. *See* 21 U.S.C. § 801 *et seq.*

40. *See* Cannabis Act, S.C. 2018, c. 16 (2018) (Can.); Carrie Khan, *Mexico Looks To Be Next To Legalize Marijuana*, NPR (November 14, 2018), https://www.npr.org/2018/11/14/667699301/mexico-hopes-to-legalize-marijuana.

41. 18 U.S.C. § 1956(a)(1), (c)(7).

42. The nexus requirement emerges out of jurisprudence regarding the extraterritorial application of U.S. criminal statutes. *See*, *e.g.*, *United States v. Lawrence*, 727 F.3d 386, 395 (5th Cir. 2013) (a federal statute may apply extraterritorially under the "protective principle", which allows a nation to "enforce criminal laws wherever and by whomever the act is performed that threatens the country's security or directly interferes with its governmental operations").

43. U.S. AML provisions may apply where the proceeds at issue are obtained directly or indirectly from an "offense against a foreign nation", such as the manufacture, import, sale, or distribution of a controlled substance, as defined under the CSA. 18 U.S.C. §§ 1956(c)(7).

44. Off. of the Comptroller of the Currency, *Corporate and Risk Governance*, at 12 (July 2016), https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf.

Matthew Biben
Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
USA

Tel: +1 212 909 6606
Email: mbiben@debevoise.com
URL: www.debevoise.com

Matthew Biben is a member of the firm's White Collar & Regulatory Defense Group and co-leads the firm's Banking Industry Group. His practice focuses on problem solving; advising organisations and individuals and investigating, negotiating and litigating complicated regulatory and enforcement matters of all types with a particular focus on matters related to financial institutions and complex situations involving the government. He has extensive experience advising boards and senior management and his enforcement and advisory work has been wide-ranging. It includes internal investigations of both domestic and international matters relating to mortgages and other consumer products and securitisation claims and data privacy breaches, False Claims Act, Anti-Money Laundering and Bank Secrecy Act work. Prior to joining Debevoise, he served for 10 years in senior in-house roles at two of the largest financial institutions.

Meryl Holt Silverman
Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
USA

Tel: +1 212 909 6889
Email: mholt@debevoise.com
URL: www.debevoise.com

Meryl Holt Silverman is a litigation associate and a member of the White Collar & Regulatory Defense Group. Her practice focuses on internal investigations, regulatory inquiries and complex civil litigation. She has briefed and argued cases in the Second Circuit and the Southern District of New York, as well as in the New York State Appellate Division, First Department and the New York State Supreme Court. Before joining Debevoise, Ms. Holt Silverman served as the New York City Corporation Counsel Honors Fellow under Corporation Counsel Zachary W. Carter from 2016 to 2017. She clerked for the Hon. Joel M. Flaum of the U.S. Court of Appeals for the Seventh Circuit from 2015 to 2016.

Debevoise & Plimpton

Debevoise is a premier law firm with a market-leading anti-money laundering and trade sanctions compliance and enforcement practice. We provide expert and practical advice to a wide range of institutions – including securities broker-dealers, asset managers, and multinational banks – as well as leading industry associations. Our attorneys draw upon extensive experience (both from the private sector and in government). We closely follow the complex and fast-changing U.S., EU and Asian AML and sanctions regimes and work with clients in all types of adversarial proceedings, ranging from contentious regulatory examinations to administrative enforcement actions to civil and criminal litigation.

Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches

Tracy French

Barbara Stettner

Allen & Overy LLP

Note

This article first appeared in the April 2018 edition of the ICLG to: Anti-Money Laundering. Below the entire article has been reproduced and updated to reflect the current state of anti-money laundering regulation of cryptocurrency in the United States and in selected jurisdictions across the globe.

Introduction

In recent years, cryptocurrencies[1] have emerged as a prominent feature of the global financial system. Since the first decentralised cryptocurrency, Bitcoin, was unveiled by the mysterious figure known only as "Satoshi Nakamoto" in 2009,[2] both the overall value of cryptocurrency in circulation and the variety of different types of cryptocurrency have expanded dramatically. According to one estimate, the global market capitalisation of cryptocurrencies exceeded USD602 billion in the fourth quarter of 2017, before falling below USD300 billion in 2018.[3]

Due to this growth, cryptocurrencies and initial coin offerings ("**ICOs**") have become an important form of personal wealth and a broad range of cryptocurrency-related businesses have emerged to serve the cryptocurrency sector. These include businesses that are directly involved in cryptocurrency trading and development, such as cryptocurrency exchanges and cryptocurrency "mining" operations,[4] as well as those that provide ancillary services to or are otherwise indirectly involved with the cryptocurrency markets and participants, including, but not limited to, firms in the retail, banking, gaming, and computing sectors. The growth of such markets has been fuelled by substantial investor interest, such that many now include cryptocurrencies within their investment portfolios.

For regulated financial institutions ("**FIs**"),[5] the opportunities presented by cryptocurrencies and distributed ledger technology ("**DLT**")[6] are tied to significant operational and regulatory challenges, not least to the implementation of anti-money laundering and counter-terrorist financing (together, "**AML**") regimes. From the regulatory standpoint, many of the risks associated with cryptocurrencies echo those presented by new financial products and technologies of the past: the risk of untested business models; the potential for abuse and fraud; the lack of a clear and shared understanding of DLT and how cryptocurrencies are sold and traded over it; and the related uncertainty of a still unshaped regulatory environment.

At the same time, key aspects of the cryptocurrency ecosystem are, by design, different from past internet-based systems and platforms. Peer-to-peer transaction authentication was created to permit coin holders to bypass institutional intermediaries, who are required to serve as essential gatekeepers in the global AML regime and in the broader financial markets. The potential for mutual anonymity among counterparties can frustrate the Know-Your-Customer ("**KYC**") and customer identification procedures ("**CIP**") on which existing AML regimes depend. The online ecosystem surrounding cryptocurrency opens new cyber and insider threat vulnerabilities, while the iterative nature of the DLT underlying cryptocurrencies prevents reversibility when a fraudulent or unlawful transaction has occurred. Finally, the absence of in-built geographic limitations makes it difficult to resolve which jurisdiction, or jurisdictions, may potentially regulate each underlying activity.

In this environment, both FIs and regulators must confront technically complex problems in a compressed time-span and in the face of what often appear to be unquantifiable risks. After an initial period of relative forbearance, financial regulators are now responding more aggressively to emerging risks and potential benefits associated with cryptocurrency, ICOs, and DLT. Recent moves by regulators in the United States and other jurisdictions to assert authority over cryptocurrency markets underscore this backdrop of legal and regulatory uncertainty. The ambiguous legal status of many cryptocurrency businesses further raises the stakes for FIs doing business with cryptocurrency entrepreneurs, whose regulatory risk tolerance may be more likely to reflect the 'wild west' culture of technology startups than that of traditional financial services providers.

Acknowledging the dynamism of the present moment, this chapter seeks to provide a high-level view of how the emerging cryptocurrency sector intersects with AML regulations and the risk-based AML diligence systems maintained by FIs. To begin, section 2 provides a brief description of how cryptocurrencies function, including the underlying technology and associated cryptocurrency businesses. Section 3 presents a non-exhaustive survey of the evolving regulation of cryptocurrency in key jurisdictions, with an emphasis on major financial centres and contrasting approaches to cryptocurrency AML regulation. Finally, section 4 identifies cryptocurrency risk considerations for FIs, focusing on risks posed by customers who hold, produce, or otherwise interact with cryptocurrencies to a significant degree and by services provided to cryptocurrency markets.

Cryptocurrency Overview

Before outlining how governments have applied AML rules to cryptocurrencies, it is helpful to establish both a basic technical understanding of how cryptocurrencies work and a common vocabulary for the types of products, services, and actors that play a role in the cryptocurrency markets.

Key Terms

Cryptocurrency is a form of virtual currency. FATF has defined "**virtual currency**" as "a digital representation of value" that "does not have legal tender status ... in any jurisdiction", and serves one or more of three functions: (1) "a medium of exchange"; (2) a "unit of account"; or (3) "a store of value".[7] Lack of legal national tender status is what, under the FATF definition, distinguishes virtual currency from "**fiat currency**", which is traditional national currency, and "e-money", which is a digital representation of fiat currency. Virtual currencies may be either convertible[8] (having a fixed or floating equivalent value in fiat currency) or non-convertible[9] (having use only within a particular domain, such as a game or a customer reward programme), and the administration of a virtual currency may be centralised[10] (controlled by a single administrator) or decentralised (governed by software using DLT principles).[11]

Under this taxonomy, a paradigmatic cryptocurrency such as Bitcoin is a convertible, decentralised virtual currency that "utilizes cryptographic principles" to ensure transactional integrity, despite the absence of trusted intermediaries such as banks. While Bitcoin, which launched in early 2009, is the oldest and most well-known cryptocurrency, many variations have since been created with various features. LiteCoin, the second-longest running cryptocurrency after Bitcoin, used the same source code but permits more efficient decryption (also known as "hashing" or "mining," as discussed below). Ether, which as of this writing has the second largest market cap after Bitcoin, debuted in 2015 and is built on a flexible "smart contract" protocol called Ethereum, which can in turn be used to encode rights in a variety of asset types into a DLT-tradable form.[12] More recent variants, such as Ripple, provide for issuance and redemption through a centralised administration controlled by a consortium of banks, while retaining decentralised exchange based on an encrypted ledger for transactions. The most recent boom has seen cryptocurrency increasingly adopted as a means of raising capital, often portrayed as a variant of "crowdsourcing" startup costs. As noted below, however, the use of cryptocurrencies to raise capital for investment purposes can raise issues under applicable securities laws and other financial regulatory regimes. Depending on the technical structure of the cryptocurrency issued, some issuers and related persons point to "utility characteristics" of the cryptocurrency (sometimes called a "coin" or "token") to argue that it is not a security under relevant case law discussed below. However, SEC Chairman Jay Clayton has cautioned that many such assertions "elevate form over substance" and that structuring a coin or token to provide some utility does not preclude it from being a security. Indeed, Chairman Clayton emphasises that a token or coin offering has the hallmarks of a security under U.S. law if it relies on marketing efforts that highlight the possibility of profits based on the entrepreneurial or managerial efforts of others, regardless of structure.[13]

Blockchain Technology

Technologically speaking, cryptocurrencies such as Bitcoin operate on the basis of a global transaction record known as a "**blockchain**". A variety of resources are available to help explain blockchain technology more thoroughly than can be done here.[14] However, at a high level, a blockchain is a particular form of DLT that requires the resolution of a new, randomised cryptographic key in order to be updated with more recent transfers. Each successive key is resolved through a process known as "**hashing**", which in practice is achieved through the ongoing computational guesswork of all computers in the network until one of the computers identifies the correct key, thus decrypting the latest iteration of the ledger (and, in the case of Bitcoin and cryptocurrencies that follow a similar model, releasing a small amount of new cryptocurrency into the world by means of a payment to the "miner" with the correct hash). Each time this occurs, the validated block of new transactions is timestamped and added to the existing chain in a chronological order, resulting in a linear succession that documents every transaction made in the history of that blockchain. Rather than residing in a centralised authoritative system, the blockchain is stored jointly by every computer node in the network. This distributed, encrypted record is what provides assurance to mutually anonymous, peer-to-peer transferees that there can be no double-spending, despite the absence of a trusted intermediary or guarantor.[15]

Blockchain has been described as "anonymous, but not private".[16] The anonymity (or "pseudo-anonymity")[17] of blockchain derives from the fact that a party transacting on the ledger is identified only by a blockchain address, which acts as an account from which value can be sent and received and can in principle be created without providing personal identifiable information. On the other hand, blockchain is not "private", since all transactions on the ledger are a matter of public record and every coin is associated with a unique transaction history. Complicating this picture, users with an interest in secrecy can employ a variety of technical tools to obscure the relationship between different blockchain addresses and actual transacting parties – while, as a countermeasure, increasingly complex data analytics methods are being developed that can identify related blockchain transactions and attribute addresses to particular users under certain circumstances.[18] The fact that even well-resourced and technically sophisticated actors face limits on their ability to decipher blockchain transactional activity, however, makes cryptocurrency attractive for money launderers and other parties seeking to exchange value away from the formal financial sector.

Cryptocurrency Businesses

Creation of a new cryptocurrency requires the development and release of the software that establishes the rules for its use, maintains the ledger, and governs the issuance and redemption of the cryptocurrency.

FATF defines a person or entity engaged as a business in putting a virtual currency into circulation and who "has the authority to redeem…the virtual currency" as the "**administrator**" of the virtual currency.[19] Many cryptocurrencies – including some of the most significant examples, such as Bitcoin, Litecoin, and Ether – have no administrator. Such cryptocurrencies are run on open-source software that governs issuance and redemption, and no central party has authority to modify the software or the rules of exchange. Other DLT applications have been developed that use the distributed ledger for validating transfers while retaining central control over issuance and redemption. The result is that the universe of "cryptocurrencies" encompasses a diverse range of virtual currencies, "coins", and "tokens" that have varying uses and characteristics and that are subject to very different degrees of control by their operators.

In addition to the creators and administrators of cryptocurrency, supporting applications have been developed to ease access and use of the underlying peer-to-peer system. In particular:

- A **Virtual Wallet** ("**wallet**") is a software application or other mechanism for holding, storing and transferring virtual currency.
  - *Custodial versus Non-Custodial*: A custodial wallet is one in which the virtual currency is held by a third party on the owner's behalf, whereas a non-custodial wallet is one in which the virtual currency owner holds his own private keys and takes responsibility for the virtual currency funds himself.

- *Hot versus Cold*: Wallet storage may be "cold", meaning held offline (usually on a USB drive) and plugged in only when needed, or "hot", meaning held online (e.g., in one of many crypto wallet applications).

- A **Virtual Currency Exchange** ("**VCE**") is a trading platform that, for a fee, supports the exchange of virtual currency for fiat currency, other forms of virtual currency or other stores of value (for example, precious metals). Individuals may use exchangers to deposit and withdraw money from trading accounts held by the VCE or to facilitate crypto-to-crypto and crypto-to-fiat exchange with the VCE or third parties through the VCE.

Whereas individual blockchain account holders may not need to involve a bank in order to obtain and transfer cryptocurrency value, the operators of these platforms frequently require traditional financial services to facilitate exchange, banking, financing, and investment with the non-crypto economy. And because the operators of these platforms typically seek to serve a large community of cryptocurrency holders for profit, they confront many of the same money laundering, fraud, cyber, and sanctions vulnerabilities as traditional financial institutions. And while the leading wallet and VCE providers use centralised data and processing models,[20] new efforts to decentralise cryptocurrency storage and exchange services create further complexity.[21] Adding to the risks, many wallet and VCE providers may, correctly or incorrectly, consider their businesses to fall outside the scope of existing AML regulations. Going forward, how to apply existing AML regimes to this complex and rapidly changing ecosystem will be a critical question for financial crime regulators.

State of Global AML Regulation

In recognition of the calls for the adoption of global AML standards for cryptocurrency trading,[22] FATF announced that it has finalised and will formally adopt as part of the FATF standards in June 2019 an Interpretive Note to Recommendation 15 to clarify how the FATF standards apply to activities or operations involving virtual assets. This should serve to reinforce what is emerging as the leading view that cryptocurrency payment service providers should be subject to the same obligations as their non-crypto counterparts,[23] and the majority of jurisdictions that have issued rules or guidance on the matter have concluded that the commercial exchange of cryptocurrency for fiat currency (including through VCEs) should be subject to AML obligations (or, in the case of China, prohibited). Salient differences in national regulations include: (i) the existence of special licensing requirements for VCEs; (ii) the extent to which AML rules also cover administrators and wallet services; (iii) the extent to which ICOs are covered by securities laws or equivalent regulations with AML regulatory implications; and (iv) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. As discussed below, in many cases the regulatory status of these activities is either ambiguous or case-specific, or is otherwise subject to pending changes in law and regulation. Note that while national security sanctions laws are outside of the scope of this article, the breadth of sanctions screening requirements will generally be equal and, more often, exceed that of AML compliance obligations.

U.S. Regulatory Approach

For purposes of U.S. federal law, a given cryptocurrency may variously be considered a currency, a security, or a commodity (and potentially more than one of these at once) under overlapping U.S. regulatory regimes. Whether particular activities involving that cryptocurrency are subject to AML regulatory obligations depends on whether the person engaging in these activities, by virtue of doing so, falls within one of the categories of "financial institutions" designated pursuant to the U.S. Bank Secrecy Act ("**BSA**").[24] The definition of "financial institution"[25] depends, *inter alia*, on registration requirements imposed by the Financial Crimes Enforcement Network ("**FinCEN**") (with respect to "money services businesses"),[26] the Securities and Exchange Commission ("**SEC**") (with respect to issuers, brokers, and dealers of securities),[27] and the Commodity Futures Trading Commission ("**CFTC**") (with respect to brokers and dealers of commodities and related financial derivatives).[28] While the regulatory framework is still emerging, these classifications potentially extend AML rules to most or all VCEs and to many cryptocurrency issuers and wallet providers. Moreover, while beyond the scope of this chapter, states can and increasingly do apply their own licensing and regulatory requirements, such as the New York State Department of Financial Services "Bitlicense" regulation.[29]

(a) Cryptocurrency Activities Triggering "Financial Institution" Status

The framework for cryptocurrency AML regulation in the U.S. is most developed for centralised VCEs. In 2013, FinCEN issued guidance concluding that "virtual currency" is a form of "value that substitutes for currency",[30] and that certain persons administering, exchanging, or using virtual currencies therefore qualify as money services businesses ("**MSB**")[31] regulated under the Bank Secrecy Act.[32] In doing so, FinCEN distinguished those who merely use "virtual currency to purchase goods or services"[33] (a "user") from exchangers and administrators of virtual currency,[34] concluding that the latter two qualify as MSBs unless an exemption applies.[35] In both cases, such a business qualifies as a covered MSB if it "(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason".[36] FinCEN has clarified in subsequent administrative rulings that this definition was not intended to cover companies' buying and selling cryptocurrencies for their own use or software developers that do not also operate exchanges.[37] The extent to which a software developer that creates the cryptocurrency that it then sells directly to users (for example, as an ICO) falls within the MSB definitions remains uncertain.[38]

Separately from FinCEN's MSB regulations, the SEC regulates transactions in securities, including by requiring issuers to register offerings of securities or to rely on an available exemption from registration. The definition of "security" under the Securities Act is extremely broad.[39] Certain tokens, including those that are effectively digital representations of traditional equity interests or debt (such as partnership interests, limited liability company interests or bonds), are plainly securities under the Securities Act. The characterisation of other tokens as securities or non-securities may be less obvious. Whether a particular instrument may be characterised as an "investment contract", and therefore a "security", is the subject of decades of SEC and SEC staff guidance, enforcement matters, and case law. In the ICO context, recent SEC speeches[40] and guidance[41] have underscored that the SEC continues to apply the analysis laid out in *SEC v. W.J. Howey Co.*[42] and the cases that followed it, specifically, whether participants in the offering make an "investment of money" in a "common enterprise" with a "reasonable expectation of profits" to be "derived from the entrepreneurial and managerial efforts of others".[43] Since first invoking this view in its investigation of the DAO ICO,[44] the SEC has taken the view that several ICOs constituted offerings of securities that failed to comply with the registration requirements of Section 5 of the Securities Act of 1933 ("**Securities Act**").[45]

While acting as a securities issuer does not make the issuer a "financial institution" under the BSA, the obligation to register a cryptocurrency as a security entails a number of Securities Act obligations,[46] and the default anonymity of cryptocurrency holders may preclude ICOs from relying on common exemptions from securities registration.[47] Furthermore, if the token offered in an ICO is deemed a security, a party that transmits tokens to purchasers on behalf of issuers or other sellers could become a securities broker-dealer for purposes of the Securities Exchange Act of 1934 (the "**Exchange Act**")[48] and accordingly be required to register as a broker-dealer subject to BSA FI obligations.[49] Similarly, when the cryptocurrencies traded are, or should be, registered as securities, a VCE may be acting as a dealer (if it acts as a market-maker for trading parties) or as a broker (a person that is in the business of effecting transactions in a cryptocurrency on behalf of others),[50] and would thus be acting as a covered FI for purposes of the BSA, absent an applicable exemption.[51]

In 2014, the CFTC observed that cryptocurrencies may constitute "commodities" under the Commodity Exchange Act ("**CEA**"), such that the CFTC has broad jurisdiction over derivatives that reference cryptocurrencies (e.g., futures, options, and swaps) and market participants that transact in such contracts. In addition, under its enforcement authority, the CFTC has asserted authority to pursue suspected fraud or manipulation with respect to the cryptocurrency itself,[52] an authority recently affirmed in federal court.[53] Persons that act as futures commission merchants ("**FCM**")[54] or introducing brokers[55] ("**IBs**") for cryptocurrency derivatives under the CEA are also covered by BSA AML requirements.[56]

(b) Consequences of Coverage

Slightly different AML programme and reporting requirements, among other things, may apply under the BSA, depending on the particular class of FI involved. However, whether qualifying as an MSB or a broker or dealer in securities or commodities, the BSA requires an FI to maintain a risk-based AML compliance programme, apply CIP, report suspicious activity and certain other transactions, and maintain certain records.[57] MSBs are further required to register with FinCEN[58] (in contrast to brokers and dealers in securities or commodities, who register with their respective regulators) and in the states where they operate, as applicable, and are subject to lower SAR filing thresholds.[59] Though the transmission of funds by MSBs does not necessarily result in the creation of a customer relationship for purposes of AML regulation, MSBs are nonetheless required to obtain identification and retain records when handling transfers of USD3,000 or more.[60] Similarly, while Currency Transaction Reporting ("**CTR**") requirements do not apply to cryptocurrency-to-cryptocurrency exchange, transactions that involve cash or equivalents for cryptocurrency would be required to be reported under these rules, including obtaining identification of the individual presenting the transaction and any person on whose behalf the transaction is made.[61]

Because FinCEN's definition of MSBs excludes registered securities and commodities brokers and dealers, the requirements specific to registered brokers and dealers prevail where cryptocurrency activities would support coverage under either prong.[62] In addition to the programmatic, reporting, and record-keeping requirements referenced above, the technical characteristics of virtual currencies could also complicate U.S. broker-dealers' efforts to fulfil their non-AML regulatory obligations in a number of ways that dovetail with challenges faced in implementing compliant AML programmes.[63]

In sum, the potential application of multiple regulatory schemes and the absence of bright line tests make ascertaining the regulatory status of particular customer types and activities labour-intensive. Many FIs are accordingly taking a conservative approach and not opening such accounts, while others have proceeded on a case-by-case basis. As the following sections illustrate, the potential for different standards and consequences to attach to cryptocurrency services that cross borders further complicates these assessments.

(c) Enforcement Trends

While many of the early enforcement actions in the United States targeting cryptocurrency businesses have involved claims of fraud[64] or failure to register with appropriate regulators,[65] there have been a few examples of enforcement actions targeting VCEs for AML programme failures and there appears to be a growing focus on AML enforcement across regulators that will inevitably extend to cryptocurrency businesses.

In May 2015, FinCEN brought its first ever action against a VCE for AML programme failures when it assessed a civil money penalty against Ripple Labs Inc. and its subsidiary XRP II LLC (Ripple) for wilful violations of the BSA's registration, programme and reporting requirements.[66] Specifically, FinCEN determined that Ripple was acting as an MSB and selling its virtual currency without registering as an MSB with FinCEN, and that it had failed to implement and maintain an adequate AML programme designed to protect its products from use by money launderers or terrorist financiers.[67] Further, Ripple failed to report suspicious activity related to several suspect financial transactions in violation of its BSA SAR-filing requirements.[68] FinCEN's press release announcing the penalty cited its 2013 guidance as having clarified the applicability of regulations implementing the BSA and the requirement to register as MSBs under federal law to virtual currency exchangers and administrators.[69] Ripple ultimately agreed to pay a USD700,000 penalty in addition to forfeiting USD450,000 to settle potential federal criminal liability,[70] and agreeing to a number of remedial actions including to only engage in its virtual currency activity through a registered MSB, to conduct a three-year look-back to identify suspicious transactions, to implement and maintain an effective AML programme, and a requirement to retain external independent auditors to review their compliance with the BSA every two years.[71]

In its second supervisory enforcement action against a virtual currency exchange, FinCEN assessed a USD110,003,314 civil money penalty against Canton Business Corporation (BTC-e), then one of the world's largest virtual currency exchanges by volume, and a USD12 million civil money penalty against one of BTC-e's Russian operators for wilful violations of the BSA and its implementing regulations in July 2017.[72] BTC-e and its operator were also indicted in federal court for violations of federal criminal AML laws.[73] FinCEN determined that BTC-e lacked basic controls to prevent the use of its platform for illicit purposes, and that the virtual currency exchange actually attracted a customer based that consisted largely of criminals seeking to launder the proceeds of their crimes.[74] In its press release announcing the penalty against the foreign-located exchange, FinCEN stated that "[r]egardless of its ownership or location, the company was required to comply with U.S. AML laws and regulations as a foreign-locted MSB including AML programme, MSB registration, suspicious activity reporting, and recordkeeping requirements".[75]

Since 2017, several individuals have faced criminal charges resulting in prison sentences for illegally exchanging and or transferring virtual currency without registering with FinCEN as an MSB. A July 2018 example involved a California woman who was sentenced to a year in prison by the District Court for the Central District of California for operating a digital currency exchange without registering with FinCEN as an MSB, and for violations of the federal criminal AML laws.[76]

Beyond FinCEN and the Department of Justice, the CFTC[77] and the SEC[78] have both taken recent actions indicating that they intend to continue to focus their enforcement authority on ensuring BSA compliance at all types of covered financial institutions subject to their supervision. In September 2018, the CFTC announced the formation of a new Bank Secrecy Act Task Force within the CFTC's Division of Enforcement, to ensure that FCMs and IBs comply with their AML obligations under the BSA.[79] While BSA requirements have applied to FCMs and IBs since 2003,[80] the CFTC has traditionally only performed the role of examiner in relation to FCM and IB compliance with the BSA, with FinCEN taking the lead in enforcement.[81] However, it appears that the CFTC now views it role in relation to BSA compliance as much broader. This new focus on enforcement could be due in part by the increasing focus on cryptocurrency regulation and the particular AML risks presented by cryptocurrency businesses, combined with the fact that the CFTC has successfully argued that cryptocurrencies are commodities subject to CFTC regulation under the CEA. Increasingly, US financial services industry regulators appear to be eager to use their enforcement mechanisms to regulate domestic and foreign cryptocurrency businesses.

European Union Regulatory Approach

The final text of the most recent European-level AML directive, the Fifth Money Laundering Directive ("**MLD5**"),[82] was published in the Official Journal of the European Union on June 19, 2018 and must be implemented by EU Member States by January 10, 2020. This is the first European Union-level money laundering directive to explicitly address the regulation of cryptocurrency.[83]

MLD5 extends the definition of "obliged entities" to include virtual currency exchanges[84] and custodial wallet providers, thereby requiring such entities to comply with the same AML requirements applied to traditional financial institutions under the EU's Fourth Money Laundering Directive ("**MLD4**")[85] – including CIP and beneficial ownership identification, KYC, transaction monitoring, and suspicious activity reporting – and subjects those entities to supervision by the competent national authorities for these areas.

While MLD5 was pending, some EU jurisdictions acted to extend AML obligations to certain cryptocurrency services on their own. As shown by the following examples, there is currently significant variation, with some Member States (such as Germany and Italy) having substantially implemented an MLD5-type regime through national law or regulatory actions, and other Member States (such as the UK and the Netherlands) having thus far left cryptocurrency trading largely outside the AML regulatory regime.

(a) Italy

When Italy amended its AML Decree[86] in compliance with MLD4 in 2017 (which was done via a legislative decree, "**AML4 Decree**"),[87] it simultaneously incorporated definitions for cryptocurrency consistent with the FATF-definition[88] and classified cryptocurrency service providers[89] that provide cryptocurrency-to-fiat conversion services as "non-financial intermediaries" regulated under the AML Decree.[90] Such service providers are consequently subject to Italian AML obligations,[91] including KYC,[92] recordkeeping and communications to the authorities,[93] suspicious transaction reporting,[94] and, as a consequence of the pseudo-anonymity of blockchain users, enhanced due diligence ("**EDD**").[95] Article 8 of the AML4 Decree further requires cryptocurrency service providers to register in a special section of the Italian Registry of currency exchange professionals[96] and to communicate to the Ministry of Economy and Finance about exchange activities carried out within the Italian territory (an issue that can be particularly complex given the decentralised, global nature of cryptocurrency transactions).[97] The Ministry of Economy and Finance published a draft decree outlining these communication requirements in February 2018, but as of this writing, the decree is still under consultation.[98]

Although Italy's investment services authority, CONSOB,[99] has not yet taken a clear position in relation to transactions in cryptocurrencies, at least one Italian court has found that the sale and conversion of cryptocurrencies to legal tender could in theory constitute a form of investment services in the context of proprietary trading.[100] A 2015 Bank of Italy communication[101] on the prudential risks of cryptocurrency further suggested that some cryptocurrency functions could violate criminal provisions of Italian banking law, which reserve certain banking, payment, and investment services exclusively to authorised entities.[102] These precedents suggest the potential for collateral risk from serving unlicensed entities or, in the extreme case, handling illicit proceeds as a consequence of serving non-compliant cryptocurrency businesses in Italy. In addition to the above, it is also worth remarking that recently (19 March 2019) CONSOB launched a public consultation with the purpose to determine the legal nature and the relevant regime applicable to the issuance or exchanges of cryptoassets. The public consultation is addressed to all entities and individuals potentially interested in cryptoassets (e.g. investors; consumers; issuers of cryptoassets; and financial intermediaries) and the term to deliver opinions and comments is set on 19 May 2019.

(b) Germany

The German Federal Financial Supervisory Authority ("**BaFin**") considers cryptocurrencies that have the character of a cash instrument to be "financial instruments" under the German Banking Act ("**KWG**").[103] However, in September 2018, this administrative practice was challenged by the Berlin Court of Appeal. The court held that Bitcoin was not a "financial instrument" and would therefore not fall under the KWG. Since BaFin is not obliged to change its administrative practice after a decision reached in an individual criminal proceeding, the future application of the KWG on cryptocurrency exchanges remains uncertain. In February 2019, the BaFin noted that it maintains its former view.

As in the U.S., use of cryptocurrency as payment for goods and services and the sale or exchange of self-procured cryptocurrency would not trigger AML regulation, and such users need not seek authorisation under applicable German banking laws.[104] However, commercial dealings with cryptocurrencies can trigger an authorisation requirement where the platform involves (i) buying and selling cryptocurrency in order to carry out principal broking services, or (ii) operating as a multilateral trading facility. Providers that act as "currency exchanges" offering to exchange legal tender for the purposes of proprietary trading, contract broking, or investment broking, are also generally subject to authorisation. Finally, underwriting an ICO may be regulated underwriting or placement business within the ambit of applicable German banking laws.

When such commercial dealings with cryptocurrencies trigger an authorisation requirement, the business must obtain a licence as a credit institution or financial services institution under applicable German banking laws, and is treated as an "obliged entity"[105] under the German Money Laundering Act ("**GWG**"),[106] transposing the MLD4 AML requirements.[107] Under the still-to-be-transposed MLD5, it is envisaged that firms operating centralised cryptocurrency exchanges or custodial wallet providers for cryptocurrencies shall also fall under the GWG. However, the legislator's planned approach to implement MLD5 in Germany and the timing for this is still unclear. It is also noteworthy that BaFin has suggested that whether a cryptocurrency

is also a security must be assessed on a case-by-case basis, with the rights associated with the respective token as the decisive factor.[108] If a token is also classified as a security (beyond the classification of a mere unit of account (*Rechnungseinheit*)), this may in particular trigger conduct and prospectus requirements that go beyond licensing requirements and a resulting AML-regulation.

(c) The Netherlands

In contrast to Germany and Italy, the Netherlands has not yet formally extended their AML regulations in order to cover cryptocurrency-related services.

The 2013 conclusion of the Dutch Ministry of Finance that cryptocurrencies are neither "electronic money" nor 'financial products' within the meaning of the Dutch Financial Supervision Act ("**DFSA**")[109] has provided assurance that virtual currencies and wallet services for currency-like cryptocurrencies fall outside the scope of the DFSA.[110] Cryptocurrencies also do not (yet) qualify as "common money".[111] Consequently, issuers of cryptocurrencies, exchange-platforms and undertakings offering wallet services are in general not covered institutions for purposes of the Dutch Act for the Prevention of Money Laundering and Financing of Terrorism ("**Wwft**").[112]

However, the Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") and the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, "**AFM**") have provided guidance regarding the qualification of cryptocurrencies as "financial instruments" as mentioned in the DFSA. In their joint advice, the DNB and the AFM concluded that currently, under Dutch law, most cryptocurrencies do not qualify as a financial instrument under the DFSA but qualify as a prepaid right to access or use a provider's future services.[113] According to the AFM, only in certain cases cryptocurrencies qualify as a "security" and hence as a "financial instrument" under the DFSA, for example, when the holder of the cryptocurrency has a right to receive dividends from the issuer of the cryptocurrency or when the cryptocurrency resembles "traditional" securities such as bonds.[114] Investment firms facilitating the trade in or providing advice regarding such cryptocurrencies qualify as "institutions" as mentioned in the Wwft. Such investment firms must meet certain obligations under the Wwft, such as conducting client due diligence and monitoring transaction performed by clients. Due to the broad definition of "client" in the Wwft and the high risks associated with cryptocurrencies, the AFM concluded that investment firms must conduct enhanced due diligence investigations regarding client-investors, but also regarding professional counterparties selling cryptocurrencies, the issuer of the cryptocurrencies and intermediaries and platforms facilitating the trade in the cryptocurrencies.[115]

When MLD5 is implemented in Dutch law, all undertakings providing exchange services between cryptocurrencies and fiat currencies which are seated in the Netherlands or offering their services to Dutch residents will fall within the scope of the Wwft. The same applies to undertakings providing custodian wallets for cryptocurrencies. The Dutch Ministry of Finance, however, does not only wish to register such undertakings as proposed in MLD5, but has proposed that such undertakings require prior authorisation from DNB before offering their services.[116] The Dutch Ministry of Finance has proposed that these undertakings should function as gatekeepers of the (Dutch) financial system. Prior to their authorisation, DNB will assess whether these undertakings are able to fulfil their role as gatekeepers by assessing whether the undertakings are able to comply with their obligations under the Wwft and by assessing the integrity and fitness of their ultimate beneficiaries and management.[117] DNB and the AFM are supporters of this licensing regime, but the Dutch Parliament has yet to vote on this proposal.

(d) The UK

In the UK, regulators have recognised that cryptoassets vary significantly both in terms of the rights they confer on their owners, as well as their designed use. Accordingly, the UK Cryptoassets Taskforce ("the **Taskforce**"), which was established in March 2018 and comprises HM Treasury, the Bank of England and the UK Financial Conduct Authority ("**FCA**"), developed a framework[118] that categorises cryptoassets into three categories:

i. Exchange tokens – these are not issued or backed by any central authority and are intended and designed to be used as a means of exchange. Examples include Bitcoin and Litecoin.

ii. Security tokens – these have specific characteristics that mean they meet the definition of a "specified investment" for the purposes of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ("**RAO**") similar to, for example, a share or debt instrument.

iii. Utility tokens – these grant holders access to a current or prospective product or service but do not typically have the characteristics of "specified investments".

The FCA confirmed in its recent consultation paper entitled "Guidance on Cryptoassets" that its prevailing view is to treat exchange tokens as falling outside the regulatory perimeter[119] and that they are not expected to be "specified investments" for the purposes of the RAO. This echoes statements made by the FCA's chief executive Andrew Bailey in 2017, that virtual "commodities" like Bitcoin are not currently regulated by UK financial regulatory authorities and that it is up to Parliament to decide on any changes to those rules.[120] Conversely, the FCA confirmed that certain tokens such as security tokens (including those issued as part of an ICO) may well constitute transferable securities and fall within the prospectus regime under the Financial Services and Markets Act 2000 ("**FSMA**"), or alternatively, depending upon how they are structured, some tokens may instead amount to a collective investment scheme under section 235 of the FSMA. Derivatives that reference a cryptoasset are also capable of being regulated investments.[121]

Unless one of the regulated financial services regimes above is triggered, cryptoasset activities are unlikely to currently fall within the scope of the UK Money Laundering Regulations 2017.[122] Changes under 5MLD (supported by the UK Treasury) would result in fiat-to-crypto exchanges and custodian wallet providers' activities being brought within the scope of AML laws. Following the work of the Taskforce, the UK government also intends to consult on broadening the UK's approach to go beyond the requirements of 5MLD to include:

- exchange services between different cryptoassets, to prevent anonymous 'layering' of funds to mask their origin;
- platforms that facilitate peer-to-peer exchange of cryptoassets, which could enable anonymous transfers of funds between individuals;
- cryptoasset ATMs, which could be used anonymously to purchase cryptoassets; and
- non-custodian wallet providers that function similarly to custodian wallet providers, which may otherwise facilitate the anonymous storage and transfer of cryptoassets.

Additionally, the UK government proposes to consult on whether to require firms based outside the UK to comply with these regulations when targeting and providing services to UK consumers. The rationale is to prevent illicit actors in the UK from dealing with firms based abroad and thereby bypassing UK regulation.

As part of developing a robust AML/CTF framework for cryptoassets, the UK government has asked the FCA to consider taking on the role of supervising and overseeing firms' fulfilment of their AML/CTF obligations in relation to crypto activities. The Taskforce's

Report notes that the UK government will consult on this before confirming the identity of the supervisor. The FCA has also taken action in relation to regulated firms who, as part of their business activities, interact with cryptoassets. In June 2018, the FCA issued a letter to CEOs of all banks, setting out appropriate practice for the handling of the financial crime risks associated with cryptoassets.[123]

On an international stage, the UK has been actively engaging in discussions to ensure a coordinated global response to the financial crime risks posed by cryptoassets. The UK continues to be a leading voice in the discussions of FATF, which continues to issue and update guidance on the AML/CTF standards that apply to cryptoassets.

Separately, where firms operate within the regulatory perimeter without correct FCA authorisation (e.g., by issuing security tokens without FCA authorisation), such breaches would be a criminal offence, and thereby may give rise to a predicate crime for certain money laundering offences under the Proceeds of Crime Act 2002 ("**POCA**"). Moreover, cryptoassets or the proceeds of their sale could also be the subject of a restraint order or confiscation order to the extent that they constitute criminal property under POCA, and concealing or handling such criminal property could trigger the money laundering offences under POCA.[124] Indeed, the recent case of *R v Teresko (Sergejs)*[125] demonstrates that the UK courts had little difficulty in concluding that Bitcoin could be the subject of a seizure order pursuant to section 47A-S of POCA.

Asia-Pacific Region

Regulatory practices in Asia diverge even more than in Europe. At the extreme end, China currently prohibits commercial issuance and exchange cryptocurrency services. In contrast, Japan and Australia both now have regimes for licensing and supervising VCEs and other cryptocurrency businesses.

(a) China

China has taken perhaps the strictest approach to cryptocurrency of the world's major economies, effectively prohibiting all issuance and exchange services for cryptocurrency in the country.

Chinese regulators took a wary view beginning in December 2013, when the People's Bank of China (the "**PBOC**"), the central regulatory authority for monetary policy and financial industry regulation, issued a joint circular with other Chinese regulators emphasising the AML risk of Bitcoin and other cryptocurrencies, and requesting that all bank branches extend their money laundering supervision to institutions that provide cryptocurrency registration, trading, and other services, and urge these institutions to strengthen their monitoring of money laundering. In 2016, a PRC-incorporated VCE platform was found partially liable for AML violations due to its failure to perform KYC while offering cryptocurrency registration and trading services.[126]

Subsequently, in September 2017, the PBOC issued a joint announcement (the "**Announcement**"), affirming that cryptocurrencies do not have legal status or characteristics that make them equivalent to money, and should not be circulated and used as currencies.[127]

- On the issuance side, the Announcement banned "coin offering fundraising", defined as a process where fundraisers distribute so-called "cryptocurrencies" to investors in return for financial contributions, and classified illegal distribution of financial tokens, illegal fundraising or issuance of securities, and fraud or pyramid schemes as financial crimes in this context. Organisations and individuals that raised money through ICOs prior to the date of the Announcement were commanded to provide refunds or make other arrangements to reasonably protect the rights and interests of investors and properly handle risks.
- On the exchange side, the Announcement required cryptocurrency trading platforms to cease offering exchange of cryptocurrency for statutory (fiat) currency, acting as central counterparties for cryptocurrencies transactions, or providing pricing, information, agency or other services for cryptocurrencies.
- In a press conference in March 2018, the former president of the PBOC Zhou Xiaochuan said that the future regulation on cryptocurrency would be very dynamic depending on the development of technology and relevant tests or evaluations.[128] However, at the current stage China is still tightening its policy in order to further eliminate illegal token fundraising, taking measures to block overseas trading platforms offering cryptocurrency exchange services to PRC residents.[129]

Because of the criminalisation of unlicensed cryptocurrency issuances, capital or fees that have been acquired through a coin release in China are likely to be viewed as illicit proceeds for purposes of both Chinese and other countries' AML laws. That said, although discouraged by the PRC authorities, individual purchase or peer-to-peer trading of crypto is not banned from a PRC law perspective.

(b) Japan

In May 2016, Japan amended its Payment Services Act to provide for a definition of cryptocurrency[130] and to create a registration requirement for "Virtual Currency Exchange Operators" ("**VCEOs**").[131] VCEO licences permit holders to engage in the exchange, purchase, sale, and safekeeping of cryptocurrencies on behalf of third parties. VCEOs are designated as "Specified Business Operators" subject to national AML rules contained in the Act on the Prevention of Transfer of Criminal Proceeds, including CIP and suspicious transaction reporting.[132] Since licences were first issued to VCEOs on September 29, 2017, the FSA, which exercises regulatory authority over Banks and other financial institutions via delegated authority from the Prime Minister, has begun conducting on-site inspections of VCEOs and has forced at least one exchange to cease operations until it remedies compliance deficiencies, including its AML compliance. The prospect of enforcement of AML regulations appears to have caused some companies to withdraw their applications to become VCEOs in recent months.[133]

(c) Australia

In Australia, cryptocurrency is regulated both as a currency and as a financial instrument such as a share in a company or a derivative depending on the features of the coin.[134] Businesses that support cryptocurrency-to-fiat exchange are classified as "digital currency exchanges" and are required to comply with the AML laws and regulations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006; however, the law was changed in 2017 to exclude most ICOs from such requirements.[135] For entities that are subject to the law, the Australian Transaction Reports and Analysis Centre ("**AUSTRAC**") has published a compliance guide for providing guidance on how to implement an AML-CTF compliance programme.[136]

Cryptocurrency Risk Considerations

Elevated AML Risks in Cryptocurrency

Cryptocurrency markets are potentially vulnerable to a wide range of criminal activity and financial crimes. Many of these risks materialise not on the blockchain itself, but in the surrounding ecosystem of issuers, VCEs, and wallets that support consumer access to DLT. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FI's subject to AML requirements to stay abreast of new criminal uses.

1. **Trafficking in Illicit Goods**: Cryptocurrencies provide an ideal means of payment for illegal goods and services, from narcotics, human trafficking, organs, child pornography, and other offerings of the "dark web". The most notable of these was the online contraband market Silk Road, in which all transactions between the buyers and sellers were conducted via Bitcoin. The site was eventually shut down by the U.S. Federal Bureau of Investigation and the founder was convicted of seven counts of money laundering, drug distribution, conspiracy, and running a continuing criminal enterprise.[137]
2. **Hacking and Identity Theft**: Crypto wallets and VCEs provide hackers with attractive targets for financial fraud and identity theft. If an account is hacked via one of these services, crypto holdings can be easily exfiltrated to anonymous accounts and liquidated for fiat or other assets, with little or no possibility of reversing or cancelling the transactions after detection.
3. **Market Manipulation and Fraud**: While the blockchain in principle allows all actors to view and monitor exchange transactions, the ability to detect and deter insider trading, front-running, pump-and-dump schemes, and other forms of market abuse involving unregistered ICOs and unlicensed VCEs is severely limited. The absence of regulatory oversight with respect to unregistered offerings and the ease with which criminal actors can create new accounts to execute manipulative schemes makes these markets vulnerable.
4. **Facilitating Unlicensed Businesses**: Variations in the legal and regulatory requirements surrounding cryptocurrency services in different jurisdictions create added challenges in determining whether cryptocurrency businesses are in compliance with local rules. Providing financial services to non-compliant entities could, in some circumstances, implicate illicit proceeds provisions.

In addition, the anonymity, liquidity, and borderless nature of cryptocurrencies makes them highly attractive to potential money launderers.

5. **Placement**: The ability to rapidly and anonymously open anonymous accounts provides a low-risk means for criminal groups to convert and consolidate illicit cash.
6. **Layering**: Cryptocurrency provides an ideal means to transit illicit proceeds across borders. For example, the U.S. Drug Enforcement Administration's 2017 National Drug Threat Assessment identified cryptocurrency payment as an "[e]merging ... vulnerability" in trade-based money laundering, in which cryptocurrency is used to transfer funds across borders in "repayment" for an actual or fictitious sale of goods. The DEA particularly identified Chinese demand for Bitcoin, helpful to avoid Chinese capital controls, creating a market for bulk fiat cash from the U.S., Europe, and Australia, with a mix of licensed and unlicensed over-the-counter Bitcoin exchanges serving as the go between.[138] Similarly, in April 2018, European authorities busted a money laundering operation that used Bitcoin purchased from a Finnish exchange to transfer cash proceeds of drug trafficking from Spain to Colombia and Panama.[139] Unregistered ICOs also provide opportunities for large scale layering. If the money launderers also control the ICO, then they can use a fraudulent "capital raising" to convert their crypto-denominated illicit proceeds back into fiat currency.
7. **Integration**: The growing list of goods accepted for purchase with cryptocurrencies expands integration opportunities. For example, the Italian National Council of Notaries recently advised notaries to make a suspicious transaction report every time they have to assist parties in the purchase of real estate by means of cryptocurrencies, since the anonymity of the crypto-payment's source would prevent the identification of the parties of the transaction.[140] The willingness of ICOs to trade crypto-for-crypto could also lead to criminal enterprises taking large stakes in crypto businesses, with or without the awareness of those businesses.
8. **Terrorism Financing and Sanctions Evasion**: The same anonymity and ease of creation makes crypto-accounts ideal for persons to receive payments that might otherwise trigger terrorism financing or sanctions red flags. Although the use of cryptocurrencies is not yet widespread in terrorism financing, terrorist groups have been experimenting with cryptocurrencies since 2014 and Bitcoin has been raised for such groups through social media fundraising campaigns.[141] States targeted by sanctions have also taken an interest in creating their own state-sponsored cryptocurrency, with Venezuela debuting such a coin in February 2018.[142]

All of these risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are signs that the cryptocurrency market is diverging, with some new coins being created to be more compatible with existing regulations while "privacy coins" prioritise secrecy of transactions and identities in order to facilitate off-market transactions.[143]

Managing Risk of Cryptocurrency Users and Counterparties

In view of the issues discussed above, financial institutions should approach services and customers connected to cryptocurrency with a full understanding of their respective roles with cryptocurrencies and any potential elevated risks. As with any new line of business, then, the central AML compliance question for financial institutions will be whether they can reasonably manage that risk. FIs that choose to serve new lines of business or customer types should perform a risk assessment so that they can tailor policies and procedures to ensure that AML obligations can still be fulfilled in the cryptocurrency context.

(a) Fulfilling Identification and Monitoring Requirements in the Cryptocurrency Context

The ability to confirm the identity, jurisdiction, and purpose of each customer is essential to the fulfillment of AML programmes. In spite of the inherent challenges that cryptocurrencies pose in all these dimensions, an FI must ensure that its policies and procedures allow it to perform these core functions with the same degree of confidence in the cryptocurrency context as they do for traditional services. While the precise measures necessary will inevitably depend on the particular customer and service, some broad points can be made.

- **Customer and Counterparty Identification**: Although the pseudo-anonymity of holders is central to many cryptocurrencies, an FI cannot enter into a customer relationship unless it has confirmed the true identity of the customer. Assuming that CIP has been performed on the customer with respect to other financial services, this is most likely to arise in the context of establishing proof of ownership over crypto-assets held by the customer outside of the FI. Similarly, although U.S. AML rules do not require FIs to perform CIP on transaction counterparties, acquisition of baseline counterparty information will typically be necessary in order to provide a reasonable assurance of sanctions compliance, as well as supporting anti-fraud and transaction monitoring efforts. In the cryptocurrency context, appropriate procedures might resemble those used to confirm ownership of non-deposit assets, such as chattel property or, even better, digital assets such as internet domains. At a minimum, the information obtained about the parties to cryptocurrency-related transactions would likely need to be sufficient to allow the FI to apply the sanctions list screening procedures it applies to other transactions of comparable risk. Since procedures should be risk-based, FIs may find it appropriate to apply more

enhanced measures to the verification of crypto-holder assets in view of the underlying risks posed by such assets.

- **Diligence/KYC, Account Monitoring, and Suspicious Activity**: The obligation to develop a reasonable understanding of "the purpose and intended nature of the business relationship"[144] generally would apply equally when that relationship involves dealings in cryptocurrency. Again, given the special concerns surrounding cryptocurrency markets, FIs may determine that heightened due diligence is appropriate in this context. Similarly, FIs may find it appropriate to develop special red flags that apply to dealings in cryptocurrency markets, and to train responsible employees accordingly.
- **Transaction Reporting and Recordkeeping**: Where covered transactions involving cryptocurrency surpass specified thresholds, FIs will need to record or report the same information as would apply for a non-cryptocurrency transaction. As with updates to CIP, the policies and procedures in place should give the FI assurance that the information that it obtains for this purpose is accurate and is sufficient for auditing review. Importantly, true identification of the holders of cryptocurrency accounts from which funds are sent and received will enable the FI to appropriately apply transaction monitoring controls, including aggregation requirements[145] and detection of structuring payments.[146] To the extent that the FI intends to rely on data analytics for these functions, such systems should be in place and tested before the FI begins processing such transactions.

(b) Assessing and Managing Risks of Customers Dealing in Cryptocurrency

Special AML considerations arise when the customer of an FI is itself a cryptocurrency business. VCE or wallet services potentially will themselves typically be classified as AML-obligated entities, depending on the jurisdiction(s) in which they offer services. A currency administrator, such as the issuer of an ICO, may also be subject to AML obligations, and all three business types may be subject to other financial services licensing or registration regimes. We outline some of these issues below.

(i) Crypto-Business Customers that Are Financial Institutions

FIs may be required to conduct additional diligence when onboarding and monitoring crypto-business customers that are themselves FIs.

In the U.S., FinCEN guidance on servicing MSB accounts drafted prior to the advent of cryptocurrency remains applicable to accounts for VCEs and wallets that are MSBs.[147] In addition to performing CIP, this guidance requires FIs to: confirm FinCEN registration status of the MSB (or application of an exemption); confirm compliance with state and local licensing requirements, if applicable; confirm agent status, if applicable; and conduct a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.[148] While an FI generally is not responsible for the effectiveness of its customers' AML programmes, deficiencies in this area can be a clear red flag when evaluating a customer's particular risk level.[149] In particular, FinCEN advises that "due diligence [of NBFI customers] should be commensurate with the level of risk...identified through its risk assessment", such that if an NBFI presents "a heightened risk of money laundering or terrorist financing, [the FI] will be expected to conduct further due diligence in a manner commensurate with the heightened risk".[150]

Onboarding and risk assessment for a cryptocurrency business is likely to encompass a number of questions related to the business' compliance with applicable regulatory requirements:

1. **Information Gathering**: Does the customer's business and compliance model permit them to collect information sufficient to perform CIP and to risk rate its own customers? To obtain information as to counterparties and the locations of transactions?
2. **Monitoring and Reporting**: Does the customer have mechanisms in place for account monitoring and procedures in place for required reporting?
3. **Geographic Controls**: Is the service able to control the jurisdictions in which its services are accessed?
4. **Legal Status and Licensing and Registration Compliance**: Has the service assessed the legality of its services in all the jurisdictions in which it operates? Has it undertaken the required licensing and registration outside the U.S.?

In some cases, cryptocurrency businesses may argue that, for legal or technical reasons, their services are not covered by the existing FinCEN registration guidance or by any state regime, and that they are therefore not required to register. These arguments may have merit in individual cases, but FIs may need to take some steps to reach their own opinion as to the validity of these assessments (particularly in cases where there is some question as to the legality of the enterprise), and may be advised to factor registration risk into their overall assessments of whether and how to provide services to the customer.[151]

(ii) Other Crypto-Business Risks

Even where an FI has assurance that the customer crypto-business is not an AML regulated entity, the FI should update policies and procedures in order to be able to account for heightened money laundering risk posed by the business.

The question of geographic control also warrants special attention in the context of servicing crypto-businesses. In addition to the risk of dealing with sanctioned persons and jurisdictions, the current absence of uniformity in the treatment of cryptocurrency activities – in particular, the differing registration requirements and the prohibition on issuance and exchange services in China – creates legal risk similar to that of online gambling or other services that are legal in some jurisdictions, but not others. The inability to control where services are offered raises the possibility that the enterprise itself is engaging in prohibited conduct. Where such prohibition is criminal, these violations could cause the crypto-business's earnings to be classified as illicit proceeds for the purposes of criminal AML provisions.[152] Regardless of whether national law applies, a strict liability approach or a knowledge/recklessness requirement to such acceptance, financial institutions' compliance programmes must include reasonable measures to detect and prevent such facilitation. Even where there is no risk of criminal violation, the FI providing services to a crypto-business should consider whether it would provide the services to a non-crypto-business whose registration status was in doubt.

Even for ICOs that do not qualify as obligated entities under relevant AML rules, FIs should carefully evaluate whether the structure of the ICO presents AML risk. An ICO should receive particular scrutiny if (i) the token sale is not capped per user, such that unlimited amounts of funds can be transferred to the ICO issuer, and (ii) the ICO intends to convert a portion of the raised funds to fiat. FIs should examine terms and conditions of an issuance to determine whether the issuer has controls in place to avoid wrongdoing.

Acknowledgment

The authors wish to thank the following attorneys for their significant contributions to this chapter: Jason Denisenko (Australia); Jane Jiang, Tiantian Wang, Jason Song, and Aubrey Tang (China); Alexander Behrens, Janis Petrowsky, David Schmid and Gero Pogrzeba (Germany); Giovanni Battista Donato, Emanuela Semino, Luca Di Lorenzi, and Amilcare Sada (Italy); Tokutaka Ito (Japan); Abas Hoesseinzada and Daphne van der Houwen (the Netherlands); Ben Regnard-Weinrabe and Heenal Vasu (UK); and Bill Satchell and Justin Cooke (U.S.).

Endnotes

1. As defined by the Financial Asset Task Force ("**FATF**"), the term "cryptocurrency" refers to any "math-based, decentralised convertible virtual currency that...incorporates principles of cryptography to implement a distributed, decentralised, secure information economy", FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 27, 2015), http://www.fatf-gafi.org/media/fatf/doc uments/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (hereinafter "FATF 2015 Guidance"). The first cryptocurrency to come into existence is called Bitcoin, and other cryptocurrencies have since been created adopting parallel principles. Cryptocurrencies may overlap to an extent with products created via so-called "initial coin offerings" or "ICOs" which are discussed further in Part 2, *infra*.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (May 24, 2009), https://bitcoin.org/bitcoin.pdf.
3. Valuations according to Cryptocurrency Market Capitalizations, https://coinmarketcap.com (last visited Apr. 4, 2018, 10:00 EST).
4. Many cryptocurrencies use a process known as "mining" to produce new crypto-coins or other cryptocurrency units. This process often involves extensive mathematical calculations, and may require significant energy and computing resources.
5. For the purpose of this article, the term "FIs" encompasses any class of persons that is obligated to undertake AML measures under the law or regulation of a particular jurisdiction. Different terms of art may be used in different jurisdictions (e.g., "financial institution", "obligated person", etc.).
6. A process through which consensus with respect to digital data replicated, shared, and synchronised across multiple nodes (or ledgers) affords confidence as to the authentication and accuracy of the shared digital data. A distinguishing feature is that there is no central administrator or centralised data storage responsible for maintaining or authenticating the accuracy of data.
7. FATF 2015 Guidance, *supra* note 2, at 26.
8. "Convertibility" means that the cryptocurrency "has an equivalent value in real currency and can be exchanged back-and-forth for real currency". As a definitional matter, FATF focuses on *de facto* convertibility – i.e., existence of a market for exchange – rather than "*ex officio* convertibility" or convertibility "guaranteed by law". FATF 2015 Guidance, *supra* note 2, at 26–27.
9. A "non-convertible" cryptocurrency is specific to a particular virtual domain or online community and does not necessarily have an established value in terms of a fiat currency. *Id*. at 7.
10. Defined by FATF as "hav[ing] a single administrating authority (administrator) – i.e., a third party that controls the system. An administrator: issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation)". *Id.* at 27.
11. Defined by FATF as "distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight". Examples include Bitcoin, LiteCoin, and Ripple. *Id.* at 27.
12. *See*, *e.g.*, Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger* (Apr. 2014), http://gavwood.com/paper.pdf (unpublished manuscript).
13. Jay Clayton, Chairman, SEC, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
14. *See, e.g.,* Jacob Kleinman, *How Does Blockchain Work?* (Jan. 16, 2018), https://lifehacker.com/what-is-blockchain-1822094625; Ameer Rosic, *What is Blockchain Technology? A Step-by-Step Guide For Beginners*, Blockgeeks (2016) https://blockgeeks.com/guides/what-is-blockchain-technology/; Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, Harvard Bus. Rev. (Jan./Feb. 2017), https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf.
15. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin Project, http://bitcoin.org/bitcoin.pdf [https://perma.cc/GXZ8-6SDR].
16. Adam Ludwin, *How Anonymous is Bitcoin?*, Coin Center (Jan. 20, 2015), https://coincenter.org/entry/how-anonymous-is-bitcoin.
17. *See*, *e.g.*, J. Luu & E.J. Imwinkelried, *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*, Criminal Law Bulletin (2016).
18. In addition to IP address concealment, users may employ so-called "mixers" or "tumblers" to exchange their Bitcoins for another set of the same value (minus a processing fee) with different addresses and transaction histories. *See* FATF 2015 Guidance, *supra* note 2, at 28.
19. FATF 2015 Guidance, *supra* note 2, at 29.
20. Examples include CoinBase and Binance.
21. For example, decentralised trading services have emerged that facilitate counterparty price communication, rather than acting as centralised market-makers, and that may facilitate brokered trades or direct peer-to-peer price trading on this basis. Examples include Herdius, AirSwap, Raiden, and Etherdelta. *See*, *e.g.*, Balazs Deme, *Decentralized vs. Centralized Exchanges*, Medium (Jan. 24, 2018), https://medium.com/herdius/decentralized-vs-centralized-exchanges-bdcda191f767.
22. *See*, *e.g.*, Steven Mnuchin, Sec'y, U.S. Dep't of Treasury, Panel Discussion at the World Economic Forum: The Remaking of Global Finance (Jan. 25, 2018) (stating that his primary goal is "to make sure that [digital currencies are] not used for illicit activities" and, to do this, he has suggested "the world have the same regulations"); Emmanuel Macron, President of France, Special Address at the World Economic Forum (Jan. 24, 2018) (calling for "a global contract for global investment").
23. FATF, *Public Statement – Mitigating Risks from Virtual Assets* (Feb. 22, 2019), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.
24. Bank Secrecy Act of 1970, as amended by the USA PATRIOT Act, 31 U.S.C. §§ 5311 *et seq*.
25. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100.
26. 31 C.F.R. § 1010.100(ff).
27. 15 U.S.C. §§ 78c(a)(4)-(a)(5).
28. 7 U.S.C. § 1a(31).
29. 23 NYCRR Part 200.
30. 31 C.F.R. § 1010.100(m).
31. The term "money services business" includes any person doing business, whether or not on a regular basis or as an organised business concern, in one or more of the following capacities: (1) currency dealer or exchanger; (2) check casher; (3) issuer of travellers' cheques, money orders, or stored value; (4) seller or redeemer of travellers' cheques, money orders or stored value; (5) money transmitter; or (6) U.S. Postal Service. Excluded from this definition are banks, foreign banks, certain SEC- and CFTC-registered persons and their non-U.S. equivalents, and persons who engage in covered activities "on an infrequent basis and not for gain or profit". 31 C.F.R. § 1010.100(ff).
32. U.S. Dep't of the Treasury Fin. Crimes Enf't Network, *FIN-2013-G001 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [hereinafter *FinCEN Guidance*]. Similar to the FATF definition, FinCEN defined "virtual currency" as a

medium of exchange that operates like a currency in some environments, but lacks attributes of real currency, such as legal tender status. FinCEN further defined "convertible virtual currency" as any virtual currency that "either has an equivalent value in real currency, or acts as a substitute for real currency". *See FinCEN Guidance* at 1–2.

33. *Id.*

34. In parallel with the FATF definitions, FinCEN defines an administrator as a business "engaged...in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency". *Id.* FinCEN defines an exchanger as a business "engaged in the exchange of virtual currency for real currency, funds, or other virtual currency". *Guidance*, *supra* note 33, at 2.

35. FinCEN's regulations provide that whether a person is a money transmitter depends on facts and circumstances. The regulations identify six circumstances in which a person is not a money transmitter, despite otherwise meeting such requirements. 31 C.F.R. § 1010.100(ff)(5)(ii)(A)–(F). As discussed below, these exemptions include instances when the entity is a registered broker or deal of commodities or securities.

36. *FinCEN Guidance*, *supra* note 33, at 3.

37. *See*, *e.g.*, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, FIN-2014-R011 (Oct. 27, 2014); Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014); Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency, FIN-2014-R007 (Apr. 29, 2014); Application of FinCEN's Regulations to Virtual Currency Software Development; and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014).

38. For a discussion of these categories, *see* Peter van Valkenburgh, *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous*, Coin Center 8 (May 20, 2017), https://coincenter.org/entry/aml-kyc-tokens. Legislation has also been proposed that would potentially extend the MSB definition to include digital wallets and cryptocurrency tumblers that merely "accept" cryptocurrency; however, the prospects of such a change are uncertain. See Senate Bill S. 1241, titled "Combating Money Laundering, Terrorist Financing and Counterfeiting Act of 2017".

39. *See* Securities Act of 1933 § 2(a)(1), 15 U.S.C. § 77b(a)(1). "The term 'security' means any note, stock, treasury stock… bond, debenture…investment contract…or, in general, any interest or instrument commonly known as a 'security'....".

40. *See, e.g.*, Jay Clayton, Chairman, SEC, *Testimony Before the Sen. Comm. on Banking, Housing, and Urban Affairs on Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission*, 115th Cong. (Feb. 6, 2018); Jay Clayton, Chairman, SEC, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

41. *See, e.g.*, *In re Munchee Inc.*, Admin. Proc. File No. 3-18304, Securities Act Release No. 10445 (Dec. 11, 2017); SEC, Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (July 25, 2017) ("DAO Report").

42. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

43. *E.g.*, DAO Report, *supra* note 42, at 13–16.

44. In the DAO investigation, the SEC found that the "reasonable expectation of profits" prong of the *Howey* test was supported by promotional materials of the issuer indicating that token purchasers would profit through the returns of the ventures to be funded by the token sales. The SEC also found that these promotional materials suggested that such returns would result from the entrepreneurial and managerial efforts of persons other than the investors, namely the issuer or others associated with it (e.g., in creating successful apps or systems or selecting profitable projects for funding).

45. *See, e.g.*, *In re Munchee Inc.*, Admin. Proc. File No. 3-18304, Securities Act Release No. 10445 (Dec. 11, 2017); DAO Report, *supra* note 42. In those cases, the SEC pointed to statements of ICO issuers – including statements in white papers related to the offering – that coin or token purchasers will profit through the returns of the venture to be funded by the coin or token sales.

46. *E.g.*, the requirement to file a registration statement that describes the cryptocurrency issuer's business operations and management, discloses potential risks of investing in the cryptocurrency, and includes recent audited financial statements for the issuer. *See* Regulation S-K, 17 C.F.R. pt. 229; Regulation S-X, 17 C.F.R. pt. 210.

47. *E.g.*, exemptions that require investors to meet certain criteria as to financial sophistication and net worth. *See, e.g.*, 17 C.F.R. §§ 230.144A, 230.500–508.

48. 15 U.S.C. § 78c(a)(5).

49. *See* 31 C.F.R. § 1010.100(t)(2) (defining a broker or dealer in securities as a "financial institution").

50. 15 U.S.C. § 78c(a)(4).

51. *See id.* §§ 78c(a)(5), 78o(b). Note that the SEC has found that certain virtual currency exchanges meet the definition of a securities exchange under the Exchange Act. *See id.* § 78c(a)(1); 17 C.F.R. § 240.3b-16(a). The SEC also applied this view in the DAO investigation, finding that the VCEs in question were exchanges because they provided users with an electronic system that matched orders from multiple parties to buy and sell DAO tokens for execution on the basis of non-discretionary methods. DAO Report, *supra* note 42, at 17. However, because a "securities exchange" is not a "financial institution" for Bank Secrecy Act purposes, no additional AML obligations attach to this determination (and, as a practical matter, such exchanges are likely to be captured by the MSB rules).

52. *See* U.S. Commodity Futures Trading Comm'n, *Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets* (Jan. 4, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf.

53. *See Commodity Futures Trading Comm'n v. McDonnell*, 18-cv-00361-JBW-RLM (E.D.N.Y. Mar. 6, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf.

54. 7 U.S.C. § 1a(28).

55. 7 U.S.C. § 1a(31).

56. *See* generally 17 C.F.R. § 42.2 and 31 C.F.R. § 1026. If an entity is engaged in: (i) soliciting or accepting customer orders for the purchase or sale of commodity-based derivatives (including cryptocurrency derivatives); and (ii) accepting customer funds, securities, or property to margin, guarantee, or secure any trades or contracts that may result from such orders, that entity qualifies as a futures commission merchant (FCM) and thus as a "financial institution" under the BSA. 31 C.F.R. § 1010.100(t)(8, 9). The BSA and related regulations require FCMs and introducing brokers to establish AML programmes, report suspicious activity, verify the identity of customers and apply enhanced due diligence to certain types of accounts involving foreign persons. The CFTC has noted that, in the future, it is possible that commodity pool operators, commodity trading advisors, swap dealers, and other CFTC registrants may be required to comply with anti-money laundering regulations; however, they are not subject to such provisions at this time.

57. 31 C.F.R. §§ 1022, 1023.

58. 31 C.F.R. § 1022.380.
59. *E.g.*, a required SAR filing threshold of USD2,000 applies to transactions by, at, or through an MSB, as opposed to USD5,000 for a broker-dealer in securities. *See* 31 C.F.R. § 1023.320; *see also* Internal Revenue Serv., *Money Services Business (MSB) Information Center*, IRS.gov, https://www.irs.gov/businesses/small-businesses-self-employed/money-services-business-msb-information-center (last visited Apr. 4, 2018).
60. 31 C.F.R. § 1010.410(e).
61. 31 C.F.R. § 1010.311.
62. 31 C.F.R. § 1010.100(ff)(8)(ii).
63. For example, difficulties in identifying and verifying customers and counterparties in the DLT context could pose challenges to the maintenance of adequate books and records. Similarly, because the funds and assets of a broker-dealer's customers must be held by a qualified custodian such as a bank or the broker-dealer itself, it may be necessary to assess whether connected wallet services meet this standard. *See* 17 C.F.R. §§ 240.15c3-3, 240.17a-3.
64. *See CFTC v. Gelfman Blueprint, Inc et al*, No. 1:17-cv-07181 (S.D.N.Y. Sept. 21, 2017) (CFTC charged Gelfman Blueprint, Inc and its CEO in the first anti-fraud enforcement action involving Bitcoin filed by the CFTC); *see also CFTC v. Dean, et al*, No. 2:18-cv-00345 (E.D.N.Y. Jan. 18, 2018) (CFTC charged a Commodity Pool Operator and its Principal for engaging in a fraudulent scheme to solicit Bitcoin from investors to be pooled and invested in various commodity interests); *see also CFTC v. McDonnell, et al*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y Mar. 6, 2018) (court held that virtual currencies are commodities under the CEA and are therefore subject to the CFTC's anti-fraud enforcement authority); *see also SEC v. PlexCorps, et al*, No. 1:7-cv-07007-DLI-RML (E.D.N.Y. Dec. 1, 2017) (SEC charged a Canadian company with fraudulently marketing tokens in an initial coin offering to US investors).
65. *See In the Matter of: BXXNA Inc d/b/a Bitfinex*, CFTC No. 16–19 (Jun. 2, 2016) (CFTC settlement order concluding that Bitfinex was operating illegally by not complying with the requirement to register as a DCM); *see also In the Matter of Munchee Inc*, Release No. 10445, Admin. File No. 3-18304 (Dec. 11, 2017) (SEC administrative proceeding brought against a California based iPhone application developer for making an illegal, unregistered securities offering in the form of an ICO); *see also SEC v. Montroll, et al.*, 1:18-cv-01582 (S.D.N.Y. Feb. 21, 2018) (SEC brought charges against an unregistered bitcoin-denominated securities and its operator for both failure to register with the SEC and also defrauding users of the exchange by misappropriating their funds).
66. *See* news release, FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (May 5, 2015) https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual (Ripple concurrently entered into a settlement agreement with the United States Attorney for the Northern District of California to resolve a criminal investigation into violations of federal law for the same underlying conduct).
67. *Id*.
68. *Id*.
69. *Id*.
70. Settlement Agreement, U.S. Dep't of Justice, U.S. Attorney, Northern Dist. of Ca (May 4, 2015) https://www.justice.gov/file/421626/download.
71. *See* endnote 66.
72. *See* news release, FinCEN 'FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales' (Jul. 26, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.
73. FinCEN, Assessment of Civil Money Penalty No. 2017-03 (Jul. 26, 2017).
74. *Id*.
75. *See* endnote 72.
76. *See* news release, Dept. of Justice, U.S. Attny's Office Central District of CA, 'Bitcoin Maven Sentenced to One Year In Federal Prison on Bitcoin Money Laundering Case" (Jul. 9, 2018).
77. The CFTC filed a complaint against 1Pool Ltd., an international trading platform, in September 2019 for engaging in unlawful retail commodity transactions (margined in Bitcoin), failing to implement procedures to prevent money-laundering, and failing to register with the CFTC.
78. The SEC issued a cease and desist order against a U.S. broker-dealer for failure to file SARs appropriately and failure to accurately document procedures set forth in its customer identification programme. The cease and desist order was issued concurrently with the announcement that the U.S. Attorney for the Southern District of New York was bringing the first ever criminal charges against a broker-dealer for violations of the BSA in connection with the same activity.
79. *See* CFTC Release No. 7809-18 (Sept. 27, 2018).
80. In 2003 the CFTC and FinCEN jointly adopted rules implementing the Patriot Act of 2001.
81. CFTC Rule 42.2 implements the authority FinCEN delegated to the CFTC to examine FCMs and IBs and ensure that they comply with the Bank Secrecy Act regulations to which they are subject, and specifically requires every FCM and IB to comply with the applicable provisions of the Bank Secrecy Act, the FinCEN regulations promulgated thereunder, and with the requirements of 31 U.S.C. 5318(l) and 31 CFR 1026.220, which require that a customer identification programme be adopted as part of the firm's Bank Secrecy Act compliance programme. Importantly, the FinCEN rule that delegates authority to the CFTC, 31 CFR § 1010.810, provides, "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter [i.e., 31 CFR Chapter X], is delegated to the Director, FinCEN" (emphasis added). The rule only delegates to the CFTC (and other financial regulators) the authority to "examine institutions to determine compliance with the requirements of" the Bank Secrecy Act.
82. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [hereinafter EU Directive 2018/843].
83. Previously, the most recent European-level AML directive, the Fourth Money Laundering Directive ("**MLD4**"), did not explicitly address cryptocurrency, and the European Commission did not interpret its then existing regulatory guidance to require extension of the MLD4 regime to cryptocurrencies. Specifically, the European Parliament and the Council of the European Union determined that the rules and regulation of the MLD4 did not apply to "providers of exchange services between virtual currencies and fiat currencies [or to] custodian wallet providers for virtual currencies". *See* Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC, COM(2016) 450 final (Oct. 28, 2016) [hereinafter Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849].
84. MLD5 defines "virtual currencies" as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally

established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically". EU Directive 2018/843, *supra* note 82.

85. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 73 [hereinafter EU Directive 2015/849].
86. Legislative Decree n. 231/2007 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (21 Nov. 2007) (It.).
87. Legislative Decree n. 90/2017 (EU MLD4) (25 May 2017) (entry into force of the new AML Decree on 4 July 2017) [hereinafter AML4 Decree] (It.).
88. Defined as "a digital representation of value, not issued by a central bank or a public authority, not necessarily linked to a currency having legal tender, used as mean of exchange for the purchase of goods and services and transferred, archived and negotiated electronically" *Id.* art. 1 ¶ 2(qq).
89. Defined as "the natural or judicial person that supplies to third parties, as a professional activity, services functional to the use, exchange, storage of crypto-currencies and to their conversion from or to currencies having legal tender" *Id.* art. 1 ¶ 2(ff).
90. *Id.* art. 3 ¶ 5(i).
91. *Id.* art. 3.
92. *Id.* arts 17–30.
93. *Id.* arts 31–34.
94. *Id.* arts 35–41.
95. Because the AML4 Decree lists anonymity as one of the factors that justify performance of enhanced KYC, cryptocurrency service providers are likely be required to implement some form of EDD when servicing pseudo-anonymous cryptocurrency accounts.
96. Held by the Italian Organization of Agents and Mediators.
97. AML4 Decree, *supra* note 73, at art. 8 (by amending Legislative Decree n.141 of 13 Aug. 2010 art. 17-*bis*.).
98. Draft of Ministry on Economy and Finance Decree on Providers of Services Relating to the Use of Crypto-Currencies, (Feb. 2, 2018), http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/regolamentazione_bancaria_finanziaria/consultazioni_pubbliche/31.01.18_bozza_DM_prestatori_val_virtuale_.pdf (It.).
99. *Commissione Nazionale per le Società e la Borsa.*
100. Legislative Decree n. 58 of 24 Feb. 1998, art. 1 ¶ 5(a) (the "Italian Financial Law") (It.). Also, note that in some cases CONSOB prohibited the activity of intermediaries offering portfolio investments in cryptocurrencies as they did not comply with formal requirements (i.e., drafting of a prospectus subject to CONSOB's approval) provided by Italian laws and regulations for the offering of financial products to the public.
101. *Banca D'Italia Eurosistem, Avvertenza sull'utilizzo delle cosiddette "valute virtuali*", 30 Jan. 2015 (It.).
102. See Legislative Decree n. 385 of 1 Sept. 1993 arts 130–131, 131-*ter*, 166 (It.).
103. Specifically, such coins are deemed to be "units of account" (*Rechnungseinheiten*). *Gesetz über das Kreditwesen* [*Kreditwesengestz*, KWG] [Banking Act], Sept. 9, 1998 at Pt. I, Div. I(1)(11). In this sense, they are distinct from legal tender and, for decentralised cryptocurrency without entitlements toward the original issuer, are not characterised as "e-money" regulated under the Payment Services Supervision Act. *Zahlungsdiensteaufsichtsgesetz* [ZAG] [Payment Services Supervision Act], Jan. 13, 2018; BaFin article about "virtual currency": https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html (*Ger.*).
104. Likewise, the creation of new cryptocurrency by solving complex mathematical computational tasks (mining) does not constitute a regulated activity according to the KWG.
105. "*Verpflichtete*".
106. *Geldwäschegesetz* [GwG] [Money Laundering Act], Aug. 13, 2008 at §§ 2(1)(1)–(2) (*Ger.*).
107. *Inter alia*, the GWG requires obliged entities to have effective risk management systems and fulfil general due diligence requirements as defined in section 10 of GWG, including customer identification, beneficial ownership identification, and risk-based diligence and account monitoring, as well as suspicious transaction reporting regardless of the value of the asset concerned or the transaction amount under section 43 of GWG. *Geldwäschegesetz* [GwG] [Money Laundering Act], *Aug. 13, 2008, §§ 10, 43 (Ger.).*
108. Fed. Fin. Supervisory Auth., *Initial Coin Offerings: Advisory Letter on the Classification of Tokens as Financial Instruments* (Mar. 28, 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1803_ICOs_en.html (*Ger.*).
109. *Wet op het financieel toezicht*, Art. 1:1 (Dutch).
110. *Beantwoording schriftelijke Kamervragen Nijboer over het gebruik van en toezicht op nieuwe digitale betaalmiddelen zoals de Bitcoin*, FM/2013/1939 U (19 Dec. 2013).
111. Court of Overijssel 14 May 2014, ECLI:NL:RBOVE:2014:2667.
112. *Wet ter voorkoming van witwassen en financiering van terrorisme*, art. 1(1) jo. 1a (Dutch).
113. DNB & AFM, *Cryptos: recommendations for a regulatory framework* (https://www.dnb.nl/en/binaries/AFM-DNB%20Crypto%20Recommendations_tcm47-381603.pdf).
114. https://www.afm.nl/en/professionals/onderwerpen/ico%20 (available in English).
115. https://www.afm.nl/~/profmedia/files/onderwerpen/wwft/wwft-cryptocurrencies.pdf (Dutch).
116. *Implementatiewet wijziging vierde anti-witwasrichtlijn*, art. 23b and further (Dutch).
117. *Memorie van toelichting Implementatiewet wijziging vierde anti-witwasrichtlijn*, p. 10–11 (Explanatory Memorandum, Dutch).
118. Cryptoassets Taskforce: final report dated October 2018.
119. FCA Consultation Paper CP 19/3 "Guidance on Cryptoassets" dated January 2019.
120. Andrew Baily, BBC's Newsnight (Dec. 14, 2017).
121. To date, the status of cryptocurrencies as constituting "money" is yet to have been challenged in the UK courts. There therefore remains a possibility that the courts would be minded to conclude in the future that cryptocurrencies, such as Bitcoin, constitute money, in circumstances where they are more commonly and continuously being accepted as payment in exchange for goods and services. Having said that, as long as a cryptocurrency is not a "fiat currency" and is not pegged to the value of a fiat currency, it is unlikely to be subject to payments regulation as currently framed in the UK.
122. I.e., the UK implementation of the MLD4.
123. "Dear CEO – cryptoassets and financial crime", FCA, 2018.
124. Proceeds of Crime Act 2002 §§ 327–329 (UK).
125. *R v Teresko* (Sergejs) (Kingston Crown Court: HHJ Lodder QC, 11 October 2017, unreported).
126. High People's Court of Heilongjiang Province of China (2016), http://wenshu.court.gov.cn/Content/Content?DocID=ce26a599-64e9-44ab-96fd-b04617d482b4 (China).

127. People's Bank of China, Ministry of Indus. & Info. Tech., State Admin. for Indus. & Commerce, China Banking Reg. Comm'n, China Secs. Regulatory Commission, & China Ins. Regulatory Comm'n, Announcement on Preventing Token Fundraising Risks (关于防范代币发行融资风险的公告), (Sept. 4, 2017), http://www.cbrc.gov.cn/chinese/home/docView/BE5842392CFF4BD98B0F3DC9C2A4C540.html (China).
128. Zhou Xiaochuan, President of the People's Bank of China, talks about "Future regulations of the cryptocurrency", http://lianghui.people.com.cn/2018npc/n1/2018/0309/c418389-29858496.html (China).
129. China's regulation of cryptocurrency and ICO: Focus of the next step, Shanghai Securities News, 23 August 2018, http://www.nbd.com.cn/articles/2018-08-23/1248158.html (China).
130. Specifically, cryptocurrency is defined as something that: (i) can be used for payment to unspecified persons in the purchase or lease of goods, or paying consideration for the receipt of the provision of services; (ii) can be purchased from and sold to unspecified persons; (iii) has financial value; (iv) is recorded by electromagnetic means in electronic devices or other items; (v) is not the currency of Japan, foreign currencies, nor an "asset denominated in currencies"; and (vi) can be transferred using electronic data processing systems. Payment Services Act, Law No. 59 of 2009, art. 2, para. 5 (Japan).
131. *See* Art. 63-5 of the Amended Payment Services Act (Japan).
132. Law No. 22 of 2007. The PTCP was amended in April 2017 to include VCEOs in this definition.
133. *More Japanese Cryptocurrency Exchanges to Close*, Nikkei (Mar. 29, 2018), https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close.
134. Australian Secs. & Inv. Comm'n, Information Sheet 225 (Sept. 2017), http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#shares (Austl.).
135. Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth); *see also* Brad Vinning & Ruby Mackenzie-Harris, *Australia: the New Digital Era: Blockchain, Cryptocurrency, and ICOs – Part 3*, Mondaq (Feb. 26, 2018), http://www.mondaq.com/australia/x/676820/fin+tech/The+new+digital+era+Blockchain+cryptocurrency+and+ICOs+Part+3.
136. Digital Currency Exchange Providers – Guidance on AML/CTF Programs, AUSTRAC http://www.austrac.gov.au/digital-currency-exchange-providers (last visited Apr. 9, 2018, 10:00 EST).
137. *See* U.S. Dep't of Justice, Press Release, Ross Ulbricht, A/K/A "Dread Pirate Roberts", Sentenced In Manhattan Federal Court To Life In Prison, (May 29, 2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.
138. Drug Enf't Admin., Dep't of Justice, 2017 National Drug Threat Assessment (DEA-DCT-DIR-040-17) 130 (Oct. 2017), https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.
139. Europol, Press Release, Illegal Network Used Cryptocurrencies and Cedit Cards to Launder More Than EUR 8 Million from Drug Trafficking (Apr. 9, 2018), https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking.
140. *See* Quesito Antiriciclaggio n. 3-2018/B, Consiglio Nazionale del Notariato (Mar. 13, 2018), http://www.dirittobancario.it/sites/default/files/allegati/quesito_antiriciclaggio_n._3-2018-b.pdf (It.).
141. Zachary K. Goldman *et al*, *Terrorist Use of Virtual Currencies*, Center for a New American Security (May 2017), https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.
142. *Venezuela Says Launch of "Petro" Cryptocurrency Raised $735 Million*, Reuters (Feb. 20, 2018), https://www.reuters.com/article/us-crypto-currencies-venezuela/venezuela-says-launch-of-petro-cryptocurrency-raised-735-million-idUSKCN1G506F.
143. For example, the cryptocurrency Monero uses "stealth addresses", which are randomly generated for each individual transaction, and "ring confidential transactions", which conceals the amount being transacted. *See* Nicolas van Saberhagen, *Crypto-Note v. 2.0* (Monero White Paper) (Oct. 17, 2013), https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf.
144. *E.g.*, FATF Recommendation 10 ("Customer Due Diligence"), https://www.cfatf-gafic.org/index.php/documents/fatf-40r/376-fatf-recommendation-10-customer-due-diligence.
145. 31 C.F.R. § 1010.313.
146. 31 U.S.C. § 5324.
147. Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (Apr. 26, 2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf.
148. *Id*. at 3 (stating that "it is reasonable and appropriate for a banking organisation to insist that a money services business provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements").
149. Fed. Fin. Insts. Examination Council, *Nonbank Financial Institutions – Overview, Bank Secrecy Act Anti-Money Laundering Examination Manual*, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_091.htm (last visited Apr. 12, 2018).
150. *Id*.
151. An ACAMs white paper has raised concerns over the phenomenon of de-risking in crypto services, and of the potential fair banking services ramifications. "While consistent regulation is lacking, [VCEs] are being denied fair banking services because they are being 'de-risked' by [FIs]. The discrimination from fair banking services VCEs are facing is comparable to the medial marijuana industry. Unlike its high-risk counterpart, Fintech innovators operate in a field that is federally legal." Sherri Scott, *Cryptocurrency Compliance: An AML Perspective, ACAMS White Paper* (n.d.), http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf.
152. FATF-modeled AML regimes include prohibitions on the acceptance of proceeds of a crime ("illicit proceeds"). *See*, *e.g.*, 18 U.S.C. §§ 1956–57.

Tracy French

Allen & Overy LLP
1101 New York Avenue, NW
Washington, D.C.
20005
USA

Tel: *+1 202 683 3866*
Email: *tracy.french@allenovery.com*
URL: *www.allenovery.com*

Tracy is an Associate in the Global Sanctions Group. Her practice focuses on economic sanctions as enforced by the U.S. Department of Treasury, Office of Foreign Assets Control ("**OFAC**") as well as anti-money laundering issues under the Bank Secrecy Act. Tracy advises global financial institutions and multinational companies on a broad spectrum of compliance and enforcement matters including internal investigations, voluntary disclosures, and the resolution of administrative and enforcement proceedings involving federal and state regulatory agencies and prosecutors. Tracy also counsels clients on anti-corruption issues and foreign investment in the United States regulated by the Committee on Foreign Investment in United States ("**CFIUS**").

Barbara Stettner

Allen & Overy LLP
1101 New York Avenue, NW
Washington, D.C.
20005
USA

Tel: *+1 202 683 3850*
Email: *barbara.stettner@allenovery.com*
URL: *www.allenovery.com*

Barbara is the Managing Partner of the Washington, D.C. office and is a member of the firm's global Executive Committee. Barbara's practice focuses on advising U.S. and foreign financial institutions on their regulatory and compliance obligations under the Securities Exchange Act of 1943, and the Bank Secrecy Act. Barbara represents global financial institutions and corporates on various financial services regulatory issues, including a strong focus on the application of anti-money laundering regimes on a cross-border basis to these global institutions.

She previously worked at the SEC's Division of Trading and Markets in the Office of the Chief Counsel and in the Office of Risk Management and Control. She also served in the Commission's Office of International Affairs together with the Financial Services Volunteer Corp, providing pro bono technical assistance to emerging markets on the creation and implementation of anti-money laundering regulations in Jordan, the UAE, Ukraine, Russia, and Romania.

ALLEN & OVERY

At a time of significant change in the legal industry, Allen & Overy is determined to continue leading the market as we have done throughout our 87-year history. To support our clients' international strategies, we have built a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in over 100 countries where we do not have a presence. This network makes us one of the largest and most connected law firms in the world, with a global reach and local depth that is simply unrivalled. Global coverage in today's market does not simply mean having offices in important cities around the world. For us, it means combining our international resources and sector expertise to work on cross-border transactions directly in the markets and regions important to our clients.

Anti-Money Laundering in the APAC Region: An Overview of the International Law Enforcement and Regulatory Framework

Nyman Gibson Miralis


Dennis Miralis


Phillip Gibson

Introduction

The Asia-Pacific or APAC region encompasses a wide range of varying jurisdictions and states including, amongst others, Australia and New Zealand in the Oceania region, Vietnam, Thailand, Malaysia, Singapore and Indonesia in South-East Asia, India and Pakistan in the subcontinent, China, Hong Kong and Japan in Eastern Asia, USA and Canada in the Americas as well as numerous Pacific Island nations. Money laundering of course is not geographically limited and illicit funds are laundered between multiple APAC jurisdictions as well as across the globe.

This chapter will examine the AML frameworks in the APAC region, encompassing both regulatory and law enforcement, with a focus on Australia's role in APAC anti-money laundering initiatives.

The Asia/Pacific Group on Money Laundering (APG) and its Role in AML

The Asia/Pacific Group on Money Laundering ('APG') is the associate Financial Action Task Force ('FAFT') member for the Asia-Pacific region. The APG operates independently under a 'Co-Chair' system of governance with both a permanent co-chair and a rotating co-chair.

Australia is a permanent APG co-chair. The chair position is currently held by Deputy Commissioner for National Security, Leanne Close of the Australian Federal Police. The present rotating chair is Bangladesh, whose chair is held by Abu Hena Mohammad Razee Hassan, head of the Bangladesh Financial Intelligence Unit. The secretariat offices of the APG are located in Sydney, Australia.

The APG consists of 41 member jurisdictions, 11 of which are also permanent members of the FATF. These core members are Australia, Canada, China, Hong Kong, India, Japan, Republic of Korea, Malaysia, New Zealand, Singapore and the United States of America. All members of the APG commit to implementing the international standards against money laundering set out in the recommendations of the FATF.

The APG monitors compliance of member countries with FATF standards. The APG also implements intergovernmental training programmes between Member States in the Asia-Pacific region.

Released on 6 September 2016, the APG *Strategic Plan 2016–2020* provides for APG's primary ongoing strategic goals namely:

1. to be an effective multilateral organisation supporting implementation of the FATF standards and the work of the global Anti-Money Laundering and Counter-Terrorism Financing network;
2. to work cooperatively to understand the risk environment for money laundering and terrorist financing and support implementation of the FATF standards; and
3. to conduct and respond to the assessment of members' compliance with, and implementation of, the FATF standards.[1]

How Does the APG Review APAC Compliance With AML Initiatives? A Survey of a Recent Mutual Evaluation

The APG mutual evaluations or 'peers review' process involves site visits conducted by rotating teams consisting of APG legal, financial and law enforcement experts. These teams attend upon the jurisdiction of fellow APG members for the purpose of testing their levels of technical compliance with AML standards, as set by the FATF, as well as anti-money laundering and counter terrorism financing effectiveness.[2]

A recent example of the mutual evaluation process was the APG onsite visit conducted on 8–19 October 2018 at Islamabad, Pakistan. The APG mutual evaluation team on this occasion consisted of:

1. Mr. Ashraf Abdulla, Maldives Monetary Authority, Maldives.
2. Ms. Jingyan Gong, People's Bank of China, China.
3. Mr. Boby Hernawan, Ministry of Finance, Indonesia.
4. Mr. James Prussing, Department of the Treasury, United States.
5. Mr. Ian Collins, New Scotland Yard, United Kingdom.
6. Mr. Mustafafa Necmeddin Oztop, Ministry of Justice, Turkey.

This team, made up of experts from APG member and observer states, conducted meetings and evaluations of various areas including government departments, governmental agencies and private sector reporting entities in the region.

The on-site visit was facilitated by the APG secretariat as well as the State Bank of Pakistan and the Pakistan Financial Monitoring Unit. The findings of this mutual evaluation process will be published in a report and presented at the 22nd APG annual meeting which is to occur in Canberra, Australia in August 2019.[3]

Since 2015, APG mutual evaluation reports have been published following APG mutual evaluation of the following jurisdictions:

1. Australia.
2. Malaysia.
3. Samoa.
4. Sri Lanka.
5. Vanuatu.

6. Canada.
7. Singapore.
8. Bangladesh.
9. Bhutan.
10. United States.
11. Cambodia.
12. Mongolia.
13. Macao, China.
14. Thailand.
15. Palau.
16. Cook Islands.
17. Indonesia.
18. Myanmar.[4]

Further to intergovernmental collaboration, the APG has also expressly provided for an increased strategic focus on information sharing and education with private sector agencies under the APG's private sector outreach programme.[5]

The United Nations Convention Against Transnational Organised Crime and the APAC Region

In addition to membership to FATF-APG, Australia and many other APAC countries are signatories to the *United Nations Convention against Transnational and Organised Crime*. Signed on 13 December 2000 and ratified on 27 May 2004,[6] the Convention includes an agreement that each state party:

1. shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasise requirements for customer identification, record-keeping and the reporting of suspicious transactions; and
2. shall ensure that administrative, regulatory, law enforcement and other authorities dedicated to combatting money laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.

The United Nations Office on Drugs and Crime ('UNODC') in the APAC Region

The UNODC operates a regional programme in South-East Asia which provides strategic oversight for Member States to combat transnational organised crime and illicit trafficking in the region by way of:

1. giving clear focus to supporting Member States and regional partners in achieving priority crime and drug outcomes in the region; and
2. increasing the responsiveness, efficiency and effectiveness of UNODC's support to the region.[7]

UNODC supports anti-money laundering capabilities in the region by facilitating collaboration with global bodies such as FATF and regional bodies including APG.

Together, the FATF standards and the UN instrument represent the key measures on which the APG and the Austrian government base their legal, regulatory and law enforcement strategy to counter money laundering.

A Recent Joint APG and UNODC Initiative on Money Laundering from Illegal Wildlife Trade

In the 2017 joint APG and UNODC research report titled *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime*, it was identified that the illegal wildlife trade is now an entranced feature of transnational organised crime with global proceeds estimated in the region of $7–23 billion USD annually.[8]

Despite the significant cash flows and transnational nature of this criminal typology, the outcomes of the research conducted highlighted multiple regulatory and law enforcement vulnerabilities in the region. For example, in many Asia-Pacific jurisdictions wildlife crime does not constitute a predicate offence to money laundering and a majority of Member States do not presently include FIU's in multi-agency anti-wildlife crime taskforces.[9]

Such findings reinforce the conclusion that international criminal organisations will continue to adapt and exploit vulnerabilities in domestic legal frameworks and regional law enforcement to launder criminal proceeds. Parallel financial investigations must accompany traditional law enforcement methods for crimes involving significant cash-flow and transnational elements.

Law Enforcement & Financial Intelligence: Key International Agencies Operating in the APAC Region

A number of law enforcement agencies operate independently and in collaboration adjunct to the regulatory Anti-Money Laundering framework established in accordance with the FATF-APG and UN instruments. Governmental examples of strategic planning, such as the *2017 Foreign Policy White Paper*, demonstrate Australia's commitment to creating a regional environment hostile to money laundering.

The section below focuses primarily on the role of Australian financial intelligence and law enforcement agencies operating within the APAC region. The Australian government anticipates continuing its leadership in promoting global standards for combatting money laundering and expressly provides for increased bilateral cooperation and diplomatic engagement with international law enforcement partners.[10]

Pacific Transnational Crime Network ('PTCN') and its role in APAC

The PTCN represents a police services-led criminal intelligence and investigation capability which operates under the governance of the Pacific Islands Chiefs of Police ('PICP') network. Developed in 2002 to combat transnational crime in the Pacific, the PTCN presently consists of 25 Transnational Crime Units from 17 Pacific Island countries.

Members include:

- Australia (Australian Federal Police).
- New Zealand (New Zealand Police).
- Samoa (Samoa Police Service).
- Fiji (Fiji Police Force).
- Solomon Islands (Royal Solomon islands Police Force).

The express purpose of the PTCN and the PICP is to build policing leadership in the Pacific region and collectively navigate regional policing challenges through discovery, knowledge, influence and partnerships.[11]

Australian Transaction Reports and Analysis Centre ('AUSTRAC') in APAC

AUSTRAC has a dual function as both Australia's specialist Financial Intelligence Unit ('FIU') and the countries anti-money laundering and counter-terrorism regulator. Tasked with identifying emerging threats and existing contraventions within the financial system, AUSTRAC's regulatory and investigative powers are set out under the AML/CTF Act and the *Financial Transactions Reports Act 1988* (Cth).

AUSTRAC primary role as a law enforcement agency is the receipt and analysis of financial data which can in turn be disseminated as intelligence to revenue, law enforcement, national security, human services, regulatory and other partner agencies in Australia and overseas.[12]

The transnational nature of money laundering practice means financial intelligence exchange among domestic agencies and international partners is essential in tracking the cross-border movements of proceeds of crime. Information shared includes transactional records, intelligence and suspicious matter reports.

Memorandums of understanding ('MoU') are presently in place between AUSTRAC and 93 other equivalent national FIU's. This includes successful agreements signed with prominent regional partners China Anti-Money Laundering Monitoring and Analysis Centre ('CAMLMAC') on 2 November 2016[13] and United States counterpart, the Financial Crimes Enforcement Network ('FinCEN') on 27 September 2018.[14]

The requirements for dissemination of information to international members of such international alliances are set out under section 132 of the AML/CTF Act. The CEO of AUSTRAC must be satisfied that:

1. the foreign government requesting the information has provided requisite undertakings as to the protection of confidential information, controlling the use of the information and assurances have been provided that the use of the information is only for the communicated purpose;[15] and
2. it is appropriate to release the information in all the circumstances.

By way of example, AUSTRAC may be empowered under the AML/CTF Act to alert one or multiple international FIU's in the event a suspicious matter report was received relating to a foreign resident. There is no requirement that such individuals be subject to investigation by Australian law enforcement agencies. Similarly, FIU counterparts in foreign jurisdictions can approach AUSTRAC directly and request the release of information held by AUSTRAC under existing information exchange programmes.

AUSTRAC provides extensive technical assistance and training programmes throughout the Asia-Pacific region to strengthen the effectiveness of counterpart FIU's. Formal training programmes focussed on capability building have been administered in Bangladesh, Cambodia, Indonesia, Nepal, Papua New Guinea, the Philippines and Thailand.[16]

The Australian Federal Police ('AFP') in the APAC region

The AFP is Australia's national law enforcement policing body, tasked with enforcing the Commonwealth criminal law including detection of contraventions of Part 10.2 Criminal Code money laundering provisions. The AFP also target related offences such as terrorism financing, offences of foreign bribery, cybercrime and tax evasion.

The AFP has demonstrated an increased strategic shift from domestic law enforcement measures towards increased international engagement. Published in 2017, the *International Engagement: 2020 and Beyond Report* recognises the need to increase collaboration with foreign law enforcement partners to combat 'the growth in criminal and terrorism threats from offshore, the continued global integration of markets and services, and the ongoing disruption of digital technologies'.[17]

The AFP describes its 'international engagement pillars' as essential in achieving its operational focus of:

1. increased strategic engagement with international partners;
2. conduct transnational operations which deliver operational effect offshore;
3. information and criminal intelligence sharing; and
4. mutual capability building.[18]

The AFP now has in excess of 300 active personnel posted in over 52 separate locations internationally including several postings with partners in Asia, South-East Asia and the Pacific catchment.[19]

In order to address offences including money laundering and transnational financial crime, the AFP has in recent times established memorandums of understanding ('MoU') with agencies in APG partner jurisdictions including the Federal Bureau of Investigation in 2015,[20] the Cambodian National Police in 2016[21] and the Chinese National Commission of Supervision in 2018.[22]

The Australian Criminal Intelligence Commission ('ACIC') in the APAC Region

The ACIC is Australia's federal criminal intelligence organisation and is mandated to combat serious and organised crime. Forming part of the Department of Home Affairs governmental portfolio, the ACIC's capabilities include:

1. Collecting criminal intelligence from partner agencies and combining it to create a comprehensive national database.
2. Utilising extensive coercive powers under the *Australian Crime Commission Act* 2002 (Cth) to obtain information.
3. Acquiring strategic intelligence products to support in decision-making, strategic targeting and policy development.
4. Implementing a national target management framework to guide law enforcement in establishing and sharing organised crime priorities and targets. This is particularly useful for dealing with multi-jurisdictional serious and organised crime investigations.[23]

The ACIC participates in a number of national law enforcement taskforces in both a formal and informal capacity. Contributing unique investigative capabilities, the ACIC provides an 'intelligence-led' response to serious and organised crime.[24]

On 21 December 2017, ACIC released the *Serious Financial Crime in Australia Report 2017*. The report acknowledged money laundering practices as one of nine key 'financial crime enablers' which effect Australia's national interests.

Money laundering is similarly identified as one of the serious organised criminal activities adversely affecting the National interests of Australia and an identified area of operations for Task Force Vestigo. Led by ACIC, the task force includes Australian Commonwealth, state and territory partners as well as Five Eyes Law Enforcement Group which comprises of law enforcement and intelligence agencies from Australia, Canada, New Zealand, the United Kingdom and the United States.[25]

While Task Force Vestigo is generalist and not limited to a specific body of criminal typology, it builds significantly on the success of the preceding Task Force Eligo, also headed by the ACIC. Commencing in December 2012, Task Force Eligo represented a collaborative special investigation into the use of alternative remittance and informal value transfer systems to launder proceeds of crime. Ultimately, by its conclusion the investigations of this inter-agency task force resulted in the seizure of in access of $580 million AUD of crime proceeds.

The Anti-Money Laundering Ecosystem: Current Examples of Multi-Agency Collaboration in APAC

Consistent with investigations such as Task Force Vertigo, there is an observable tendency for FIU's, Federal and State law enforcement, governmental non-law enforcement agencies and private bodies to formalise collaborative engagements in response to the shifting criminal environment.

Contemporary examples of multi-agency responses operating in the Asia-Pacific region include:

The Serious Financial Crime Taskforce ('SFCT')

An Australian multi-agency taskforce which includes:

- AFP.
- Australian Tax Office ('ATO').
- Australian Crime Commission ('ACC').
- Attorney-General's Department ('AGD').
- AUSTRAC.
- Australian Securities and Investments Commission ('ASIC').
- CDPP.
- Australian Border Force ('ABF').

The Egmond Group

A global network of 156 FIU's committed to collaboration and information exchange. Notable Asia-Pacific members include:

- AUSTRAC.
- Hong Kong SAR, China Joint Financial Intelligence Unit ('JFIU').
- Indonesian Financial Transaction Reports and Analysis Centre ('PPATK').
- Anti-Money Laundering Office Thailand ('AMLO').

The Fintel Alliance

Led by AUSTRAC, Fintel is a public-private partnership aimed at combatting money laundering and terrorism financing. Members include:

- Commonwealth Bank of Australia.
- National Australia Bank.
- Australia and New Zealand Banking Group.
- Westpac.
- Paypal.
- Western Union.
- NSW Police Force.
- ATO.
- National Crime Agency (UK).

Money Laundering Typologies: A Diverse Range of Criminal Activities

In order to better understand and combat the risk environment for money laundering and terrorist financing in the Asia-Pacific, the APG engage in and disseminate typologies research. This study of methods, techniques and trends of money laundering and terrorism financing offers a valuable toll to understand and classify money laundering and areas of associated risk.

What Are Some Recent APAC Money Laundering Typologies?

The *APG Yearly Typologies Report 2018* identifies the numerous typologies used to launder proceeds of crime in the Asia-Pacific region. These typologies have been identified following an evaluation of case studies which reflect the present and emerging money-laundering landscape in Afghanistan, Australia, Bangladesh, Brunei, Fiji, Hong Kong, Japan, Lao, Macao, Malaysia, New Zealand, Pakistan, Philippines, Singapore, Chinese Taipei and Thailand.[26]

1. Cash conversion & currency exchange

The use by criminals of travellers' cheques, stored value cards or currency exchange houses to transport money between jurisdictions without direct transfer of funds. The use of cash smugglers is also common in efforts to conceal the movement of currency.

The proliferation of bitcoin and other cryptocurrencies has also shown an increase in the illegal used of digital currencies in preference to traditional currencies. This is due to the mediums perceived anonymity and market volatility.

Smart Automatic Teller machines have also been used to make high volumes of illegal cash deposits to third-party accounts while avoiding direct interaction with banking staff.

2. Corruption associated money laundering

The use of bribery of public officials and private sector compliance staff to undermine anti-money laundering regulation and reporting measures.

This method may also involve the use of corrupt 'gatekeeper' professionals including bankers, lawyers, accountants and brokers who succumb to coercion on the part of criminals or alternatively actively market specialist methods of laundering money.

3. Structuring

Also known as 'smurfing', this method involves a high volume of comparatively small transactions between multiple parties and accounts to avoid detection threshold reporting obligations.

Difficulty in detection is increased by virtue of the involvement of persons unaware of their participation in such schemes, which involve what would otherwise be a series of legitimate financial transactions.

4. Use of portable commodities

The purchase of high-net-value instruments such as jewellery, diamonds, precious metals, race horses and illicit drugs are used to conceal net worth and property ownership as well as a means of transporting assets through international points of entry without detection or reporting.

Commodity exchange or barter of such items between parties also can be used to avoid the use of private reporting entities such as banks. The transnational trade of child pornography, for example, has also been subject to prosecution for money laundering offences in Australia.[27]

5. Use of wire transfers

Electronic wire transfers between banks financial institutions can be used both as a method to avoiding detection but also as a means to avoid confiscation of proceeds of crime by rapid removal of funds from jurisdictions seeking to enforce anti-money laundering measures.

6. Alternative remittance services: Hawala, Hundi, etc.

Such services are identified as underground or unregulated networks of trust-based, intra-jurisdictional transfers used to remit monies. Such methods are commonly used by money launders parallel to the traditional banking sector.

Alternative remittance providers increase the difficultly by which law enforcement and FIU's can identify individuals or parties controlling funds, as well as obscuring the observable transferor-transferee relationship.

7. Gambling and gaming activities

Such methods exploit the high-net-value of assets which are held and pass between parties in the gambling sector. Examples include use of online gambling or online gaming accounts to conceal overall value of assets held, the use of winning tickets to conceal crime proceeds and use of casino chips as currency.

8. Invoice Manipulation

Both over- and under-invoicing of goods or services can be used in conjunction with import and export activities to obscure movement of funds between international jurisdictions and disguise illegitimate wealth as traditional trade activity.

Such a method is often used in tandem with complex transnational business structures to conceal the identities of individuals involved.

9. Business investment or 'Mingling'

As one of the key objectives of money laundering activity, 'mingling' involves the deliberate combining of proceeds of crime with profits from legitimate business enterprise to obscure the source of funds and perpetuate the impression of 'clean' money.

The practice may be combined with false accounting practices to manipulate the observable proportions of profit obtained through legitimate enterprise.

10. Identity fraud and false identification

Identity fraud can be used both a method of concealment to engage in separate money laundering typologies or as a means of obtaining further illegitimate funds through welfare fraud, superannuation fraud, obtaining fraudulent cash loans or lodgement of false tax returns.[28]

In the ACIC's *Serious Financial Crime in Australia Report 2017*, it was identified that the methodology used to launder proceeds of a crime is also influenced by the area of crime the proceeds originate from. The proceeds of a drug crime, for example, commonly requires large amounts of illegally obtained cash to be deposited into the banking system. Alternatively, financial or 'white-collar' crime often involves the manipulation of accounting practices for money already contained within legitimate banking systems.[29]

Irrespective of the original source of the funds, the use of global methods and prevalence of transnational transfers to launder proceeds of crimes, as well as the increased use of technology to enable and conceal financial crime, make up entrenched features of money laundering in the Asia-Pacific region. Such enablers are the subject of increased anti-money laundering attention, investment and collaboration from law enforcement agencies and their partners.

Recent Media Publications by Asia-Pacific Law Enforcement Relating to Money Laundering Activity

Strike Force Bugam

Strike Force Bugam represented a joint agency investigation conducted by the NSW Police Organised Crime Squad and the ACIC which culminated in the arrest and prosecution of numerous persons said to be involved in internationally-based money laundering syndicate, operating out of Sydney between 2016 and 2017.

The execution of six separate search warrants on 7 November 2017 and two further search warrants on 29 November 2017 resulted in the seizure of cash, documentation, mobile phones, firearms, motor vehicles, a boat and prohibited drugs.[30]

A resident of Dee Why, NSW was charged with the State offences of knowledge of direct activities of a criminal group, participating in a criminal group, drug supply, drug possession, knowingly dealing with proceeds of a crime, publishing false misleading material to obtain advantage, receiving vessel/part-theft, disposing vessel/part-theft, knowingly possessing an identity plate on an incorrect vehicle and dishonestly possessing and interfering with a unique identifier.

A resident of Lidcombe, NSW was charged with the State offences of participating in and contributing to a criminal group, dealing with property proceeds of crime, knowingly dealing with the proceeds of a crime, dishonestly interfering/copying a unique identifier, dishonestly possessing and interfering with a unique identifier, disposing of a vessel/part-theft and knowingly facilitating an organised car re-birthing activity.

In total, $1.7 million AUD in currency, 12.25kg cocaine, 6.2kg of methamphetamine, 1,000 MDMA tablets and seven firearms were seized. The resulting arrest and prosecution of 18 persons is alleged to have dismantled three related criminal syndicates and resulted from intelligence sharing and money-tracing investigations conducted between the NSW Police and the ACIC.[31]

These investigative activities also resulted in regulatory action being taken against the Commonwealth Bank by AUSTRAC in response to the banks alleged failure to report transactions made using Commonwealth Bank smart deposit machines.[32]

It is estimated by AUSTRAC that the criminal syndicates had engaged in an operation which had laundered in excess of $42 million AUD for international crime groups.

Strike Force Mactier

Strike Force Mactier represented targeted, collaborative investigations into international money laundering by officers and staff of the NSW Police Force, the NSW Crime Commission, AFP, and the ABF.[33]

A series of arrests were made between 5 November 2018 and 16 November 2018 at the Sydney International Airport, Sydney CBD and Bondi Junction. Five Hong Kong nationals were charged with offences including recklessly dealing with the proceeds of a crime, knowledge of direct activities of a criminal group, contributing to criminal activity and participating in a criminal group.

A total of $180,000 AUD currency, SIM cards and mobile phones were seized during subsequent search warrants.

It is alleged that the persons were laundering money within Australia before transferring funds offshore into Hong Kong and mainland China.

AFP – Chinese Ministry of Public Security ('CMPS') Joint Operation

Between 14 and 15 November 2018, AFP officers performed search warrants on residential homes located in Sydney, NSW Melbourne, VIC and the Gold Coast, QLD in response to a request for assistance in 2016 made to the AFP by the CMPS.

During the course of these search warrants, investigators seized jewellery, vehicles and other property valued in excess of $8.5 million AUD. It is alleged that Chinese nationals had established shell companies in Australia to purchase extensive residential and development property, using funds illegally acquired in China through fraudulent investment.[34]

While no criminal proceedings were instigated against the Chinese nationals subjected to the search warrants, an application for a restraining order was made under *Proceeds of Crime Act 2002* for the related Commonwealth indictable offence of dealing with proceeds of crime contrary to section 400.3 of the Criminal Code as well as fraud and tax evasion offences.

Overview of Laws in Australia

In accordance with Australia's obligations as an APG member and signatory to the *United Nations Convention against Transnational and Organised Crime*, money laundering activities and dealing with the proceeds of crime are criminal offences in Australia.

Criminal Code Act 1995 (Cth)

Money laundering is an offence prohibited at a Federal level under Part 10.2 of the Criminal Code Act 1995 (Cth) ('Criminal Code'). The provisions cover a wide variety of offending conduct relating to money, or other property, that is used in connection with serious crime. This legislative regime has been described judicially as a '21st century response to antisocial and criminal conduct, commonly with international elements'.[35]

Sections 400.3–400.9 of the Criminal Code include offence provisions which make it an offence to deal with or receive, possess, conceal, dispose, import, export or engage in a banking transaction relating to money or property which represents proceeds or an instrument of crime.[36]

Property will be classified as *proceeds of crime* under the Criminal Code if it is wholly or partly derived or realised (directly or indirectly) by any person from the commission of an indictable offence against a law of the Commonwealth, a State, a Territory or a foreign country.[37]

Property will be classified as an *instrument of crime* if it is used in the commission of, or used to facilitate the commission of, an indictable offence against a law of the Commonwealth, a State, a Territory or a foreign country.

Commonwealth and State indictable offences, which may constitute a predicate offence for the purpose of money laundering, include tax evasion, fraud, bribery and corruption offences as well drug importation, manufacture or supply.

The fault element is established under the offence provisions by proving intention, knowledge, recklessness or negligence on the part of the accused person to the fact that they were dealing with the proceeds of a crime or an instrument of a crime.

The corresponding maximum penalties for offences set out under Part 10.2 of the Criminal Code vary based on the value of the property dealt with and the fault element demonstrated on the part of the accused person.

By way of example, if the prosecution can establish beyond reasonable doubt that an accused person deals with money or property that the person believes to be proceeds of a crime (or intends for the property to become an instrument of crime) and the property is valued at $1,000,000 AUD or more, the person is liable to a maximum term of imprisonment of 25 years and or a fine of up to $315,000 AUD.[38]

The offence provision has extraterritorial jurisdiction in that is not restricted to application against Australian nationals or persons residing in Australia. Foreign nationals can be prosecuted if proceeds of a crime are dealt with in Australia or the conduct which constitutes the relevant indictable predicate offence is an Australian Commonwealth, State or Territory offence.

Proceeds of Crime Act 2002 (Cth)

As of 1 January 2003, the AFP and the Commonwealth Director of Public Prosecutions ('CDPP') have been empowered under the *Proceeds of Crime Act 2002* ('POCA') to seek restraining, forfeiture or freezing orders in relation to property suspected of being connected with a criminal offence.

Typically, assets including actual, real and interests in property, becomes subject to an order if it is established that the property is suspected on reasonable grounds to be the proceeds of an indictable offence, a foreign indictable offence or was previously used in connection with the commission of an offence.[39]

A Court must also make an order that property subject to the application be forfeited to the Commonwealth if a person has been convicted of one or more indictable offences and the court is satisfied that the property is proceeds or an instrument of one or more of the offences.[40]

It is an express object of POCA to give effect to Australia's obligations under the Council of Europe *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*, and other international agreements relating to proceeds of crime.[41]

Anti-Money Laundering Counter-Terrorism Financing Act 2006 (Cth)

The conduct of financial institutions in Australia is regulated under the *Anti-Money Laundering Counter-Terrorism Financing Act* 2006 (Cth) ('AML/CTF Act'). The AML/CTF Act sets requirements for reporting entities including institutions within the financial sector, gambling sector and business involved in the trade of bullion.[42]

Obligations are imposed on reporting entities including a requirement to:

1. enrol and register businesses conducting relevant business;[43]
2. conduct due diligence on all customers including confirmation of identity;[44]
3. retain transaction records for a period of seven years;[45]
4. develop and implement programmes for the detection of money laundering activity;[46] and
5. report suspicious matters to the ('AUSTRAC').[47]

AUSTRAC is Australia's primary financial intelligence unit. AUSTRAC also functions as the national regulator under the AML/CTF Act. The roles and responsibilities of AUSTRAC are covered in further detail below.

A majority of the penalties imposed for non-compliance with the AML/CTF Act are civil and not criminal in nature. An established breach of a civil penalty provision under AML/CTF Act can attract significant monetary penalty, with maximum fines of $21 million AUD per offence applying under the legislation.

Some contraventions under the AML/CTF Act do attract criminal sanctions. It is a criminal offence to provide a designated service under a false name[48] or conduct transactions with the intention of avoiding reporting requirements.[49] Further 'tipping off' offence provisions prohibit contact or communication with persons, other than AUSTRAC personnel, following a referral of suspicious activity. For example, it is a criminal offence under such a provision for a reporting entity such as a bank to notify AUSTRAC of suspicious activity on the part of a customer while simultaneously notifying the relevant customer that their conduct has been reported to AUSTRAC.

The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017* was passed by both houses of Parliament on 7 December 2017 and commenced on 3 April 2018. This amending legislation expanded AUSTRAC's powers under the AML/CTF Act to monitor digital currency markets. As with existing reporting entities within the finance sector, digital currency exchange providers are now required to register under the AML/CTF Act and comply with the obligations set out under the Act.[50]

The legislative amendment follows a growing acknowledgment among members of the FATF and APG that digital currency providers present elevated risks as facilitators of criminal activity including money laundering, cybercrime and terrorism financing activities.

Australia's legislative amendments follow comparable recent regulatory action on the part of the Hong Kong Regulatory Authority, Bank of Negara Malaysia and the Monetary Authority of Singapore.[51] In these jurisdictions, the amendments bring cryptocurrencies and providers of digital currency predominantly in line with traditional financial and property exchange markets, for the purpose of anti-money laundering regulation.

Political focus on legislative regulation of transitional financial crime has intensified in the region. In the lead up to the 2019 Federal election in Australia, shadow treasurer Chris Bowen has levelled criticisms at the existing coalition government for its delay in implementing Tranche 2 laws, a proposed further amendment of the AML/CTF Act extending the compliance measures to non-financial sectors in which vulnerability have been established. Such sectors include the real estate industry as well as the legal and accounting professions.[52]

The criticism follows recent media coverage including the ABC's Four Corners 'Project Dragon' investigation, aired 18 February 2019, which revealed rising concerns from the Chinese Government about the growing import and export of illicit funds by Chinese nationals in Australia. The investigation revealed the increasingly prevalent practice of private 'bounty hunter' engagement by Chinese government agencies in which civil agents are used to recover Chinese proceeds of crime currently held in Austrian markets.[53]

Conclusion

To create an environment hostile to money laundering efforts in the APAC region, APG and its partner agencies will continue to collaborate and build the capability of regional partners to ensure the standards of the FATF are met and effectively enforced. The increase in FATF compliant Member States in the APG region will decrease the number of 'soft targets' presently exploited by criminal syndicates in the region.

It is predicted that FIU's and law enforcement agencies in the Asia-Pacific region will continue a deliberate shift away from 'as necessary' international collaborative operations and increasingly operate within proactive inter-agency action groups to address serious transnational financial crime and money laundering. Australia will also continue its efforts in formalising mutual assistance agreements with Asia-Pacific partners and increase its physical presence throughout the region, in recognition of the increasingly global nature of financial crime.

Endnotes

1. Asia/Pacific Group, *Strategic Plan 2016–2020*, 2016, Sydney, p. 11.
2. Asia/Pacific Group, http://www.apgml.org/mutual-evaluations/page.aspx?p=a901712a-54e4-4b3b-a146-046aefca6534, accessed 12 March 2019.
3. Asia/Pacific Group, http://www.apgml.org/mutual-evaluations/news/details.aspx?pcPage=1&n=1137, accessed 12 March 2019.
4. Asia/Pacific Group, http://www.apgml.org/mutual-evaluations/page.aspx?p=c12cf2af-4e56-472c-9201-90d0baf9ceda, accessed 12 March 2019.
5. Asia/Pacific Group, *Strategic Plan 2016–2020*, 2016, Sydney, p. 8.
6. *United Nations Convention on Transnational Organised Crime*, GA Res 55/25, 2000.
7. https://www.unodc.org/southeastasiaandpacific/en/what-we-do/index.html.
8. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime*, 2017, Sydney, p. 5.
9. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime, 2017*, Sydney, p. 6.
10. Australian Government, *2017 Foreign Policy Whitepaper*, 2017, Canberra, p. 73.
11. Pacific Islands Chiefs of Police, https://picp.co.nz/about-pacific-islands-chiefs-of-police-picp/vision-purpose-strategy/, accessed 11 March 2019.
12. Miralis, D & Gibson P 'Australia: An increasingly global approach' *Global Investigations Review*, 17 September 2019, p. 4.
13. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/media/media-releases/austrac-signs-historic-mou-china, accessed 7 March 2019.
14. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/media/media-releases/australia-strengthens-international-partnerships-fight-against-financial-crime, accessed 7 March 2019.
15. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), s. 132(1)(a).
16. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/about-us/international-engagement/international-assistance-and-training, accessed 7 March 2019.
17. Australian Federal Police, *International Engagement: 2020 and Beyond Report*, 2017, Canberra, p. 4.
18. Australian Federal Police, *International Engagement: 2020 and Beyond Report*, 2017, Canberra, p. 4.
19. Miralis, D & Gibson P 'Australia: An increasingly global approach' *Global Investigations Review*, 17 September 2019, p. 4.

20. SBS News, https://www.sbs.com.au/news/afp-fbi-pool resources-against-crime, accessed 7 March 2019.
21. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/afp-and-cambodian-authorities-working-closely-combat-drugs-and, accessed 7 March 2019.
22. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/australia-re-signs-landmark-deal-china, accessed 7 March 2019.
23. Nyman Gibson Miralis, https://ngm.com.au/money-laundering-lawyers/money-laundering-australian-crime-commission-investigations/, accessed 7 March 2019.
24. Australian Criminal Intelligence Commission, https://www.acic.gov.au/about-crime/task-forces, accessed 7 March 2019.
25. Australian Criminal Intelligence Commission, https://www.acic.gov.au/about-crime/task-forces/vestigo-task-force, accessed 7 March 2019.
26. Asia/Pacific Group, *APG Yearly Typologies Report 2018: Modern Trends of Money Laundering and Terrorism Financing*, 2018, Kathmandu.
27. *Dennison v R* [2011] NSWCCA 114.
28. Asia/Pacific Group, http://www.apgml.org/methods-and-trends/page.aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da, accessed 7 March 2019.
29. Australian Criminal Intelligence Commission, *Serious Financial Crime in Australia Report 2017*, Canberra, p. 12. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime, 2017*, Sydney, p. 5.
30. Australian Criminal Intelligence Commission, https://www.acic.gov.au/media-centre/joint-media-releases/joint-investigation-dismantles-sydney-based-alleged-criminal-syndicate, accessed 7 March 2019.
31. Australian Criminal Intelligence Commission, https://www.acic.gov.au/media-centre/joint-media-releases/joint-investigation-dismantles-sydney-based-alleged-criminal-syndicate, accessed 7 March 2019.
32. Australian Financial Review, https://www.afr.com/news/politics/cba-customers-named-in-strike-force-bugnam-20171218-h06dcf, accessed 7 March 2019.
33. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/five-charged-and-180000-seized-over-alleged-international-money-laundering, accessed 7 March 2019.
34. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/afp-operation-targets-chinese-nationals-allegedly-laundering-proceeds, accessed 7 March 2019.
35. *R (Cth) v Milne (No 1)* [2010] NSWSC 932 at [164].
36. *Commonwealth Criminal Code Act 1995* (Cth), s. 400.2.
37. *Commonwealth Criminal Code Act 1995* (Cth), s.400.1.
38. *Commonwealth Criminal Code Act 1995* (Cth), s.400.3.
39. See *Proceeds of Crime Act 2002* (Cth) ss. 15B; 329.
40. *Proceeds of Crime Act 2002* (Cth) s. 48.
41. *Proceeds of Crime Act 2002* (Cth) s. 5.
42. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/businesses/legislation/amlctf-act, accessed 7 March 2019.
43. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 7.
44. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 28.
45. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 107.
46. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 81.
47. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 41.
48. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 139.
49. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), s. 142.
50. *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017* (Cth), Part 2 s. 4.
51. Deloitte, *Asia Pacific Regulatory Update*, 2018, Sydney, p. 1.
52. JD Supra, https://www.jdsupra.com/legalnews/financial-crime-set-to-become-a-pre-47276/, accessed 11 March 2019.
53. JD Supra, https://www.jdsupra.com/legalnews/financial-crime-set-to-become-a-pre-47276/, accessed 11 March 2019.

Acknowledgment

The authors would like to thank Jasmina Ceic for her invaluable contribution to the writing of this chapter. Jasmina is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system.

(Tel: +61 2 9264 8884 / Email: jc@ngm.com.au)

Dennis Miralis
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, cybercrime, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.

Phillip Gibson
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions often involving: white-collar and corporate crime; assets forfeiture; money laundering and proceeds of a crime; extradition; mutual assistance; Royal Commissions; bribery and corruption; and ICAC and Crime Commissions matters. He has extensive experience in dealing with all major Australian and international investigative agencies.

NYMAN GIBSON ngm MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, cybercrime, international asset freezing or forfeiture, extradition and mutual assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

Australia

Kate Jackson-Maynes

King & Wood Mallesons

Amelia Jamieson

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering is a criminal offence under Part 10.2 of the *Criminal Code Act 1995* (Criminal Code). The Commonwealth Director of Public Prosecutions (CDPP) is the primary authority responsible for prosecuting money laundering offences. There are also money laundering offences at the State and Territory level which are prosecuted by authorities in the States and Territories.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

A person commits a money laundering offence under the Criminal Code if they "*deal*" with money or property and the money or property is (and the person believes that it is) the *proceeds of crime* or the person intends that the money or property will become an *instrument of crime*. "*Dealing*" includes receiving, possessing, concealing, disposing of, importing or exporting the money or property, or engaging in a banking transaction relating to the money or property.

It is also an offence if the person "*deals*" with money or property and:

- the person is reckless or negligent as to the fact that the money or property is *proceeds of crime* or there is a risk that it will become an *instrument of crime*; or
- it is reasonable to suspect that the money or property is *proceeds of crime*.

For a person to be found guilty of committing a money laundering offence under the Criminal Code, the government must prove the physical and fault elements of the offence beyond reasonable doubt. The physical element is that the dealing took place and the fault element is that the person had the requisite intention, knowledge, recklessness or negligence.

For money or property to be the *proceeds of crime*, it must be wholly or partly derived or realised (directly or indirectly) by any person from the commission of an indictable offence against a law of the Commonwealth, a State, a Territory or a foreign country. For money or property to be an *instrument of crime*, it must be used in the commission of, or used to facilitate the commission of, an indictable offence against a law of the Commonwealth, a State, a Territory or a foreign country.

Under the Criminal Code, a Commonwealth offence may be dealt with as an indictable offence if it is punishable by imprisonment for a period exceeding 12 months.

For example, the crime of tax evasion is generally prosecuted as one or more of the fraud offences under Part 7.3 of the Criminal Code, which are punishable by imprisonment for five years or more (making it an indictable offence). There are also other offences relating to tax evasion under other Commonwealth, State and Territory legislation and a number of those offences are punishable by imprisonment for 12 months or more. Accordingly, tax evasion is likely to be a predicate offence for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes. The offence of money laundering has extraterritorial application under the Criminal Code.

For Australian citizens, Australian residents or Australian bodies corporate, the offence generally applies to all conduct of those persons inside or outside Australia. For all other persons, the relevant geographical link will generally only be established if:

- the conduct that constitutes the money laundering offence (i.e. the "*dealing*" with money or property) occurs wholly or partly in Australia; or
- the conduct that constitutes the predicate offence is a Commonwealth, State or Territory indictable offence (not a foreign offence).

For example, a foreign person may commit a money laundering offence under the Criminal Code if the predicate offence is a foreign crime but the "*dealing*" with the proceeds of the foreign crime occurs in Australia.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

See the response to question 1.1 above.

A number of government bodies may investigate and refer money laundering offences to the CDPP, including the Australian Federal Police (AFP), the Australian Taxation Office and Australian Transaction Reports and Analysis Centre (AUSTRAC). State and Territory bodies may also refer matters to State and Territory prosecution authorities.

1.5 Is there corporate criminal liability or only liability for natural persons?

Corporate criminal liability exists in Australia. The Criminal Code applies to bodies corporate in the same way as it applies to individuals. A body corporate can therefore be convicted of a money laundering offence under the Criminal Code. The principles relating to the fault element and physical element of the offence that must be proved in respect of bodies corporate are set out in Part 2.5 of the Criminal Code.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalties for money laundering offences vary depending on the value of the money or property that has been dealt with and the degree of knowledge of the offender. For individuals, the maximum penalty under the Criminal Code is 25 years of imprisonment and a fine of A$315,000 (i.e. 1,500 penalty units) for an offence of dealing with the proceeds of crime which have a value of A$1,000,000 or more, where the person believes the money or property to be the proceeds of crime. For bodies corporate, the maximum penalty for the same offence is a fine of A$1,575,000 (see *Crimes Act 1914* section 4B).

1.7 What is the statute of limitations for money laundering crimes?

There is generally no time limit for prosecutions of money laundering offences under the Criminal Code (see *Crimes Act 1914* section 15B). There is a time limit for the CDPP to bring proceedings (one year after the commission of a money laundering offence) where the maximum term of imprisonment for an individual is six months or less or the maximum penalty for a body corporate is 150 penalty units or less (these are generally money laundering offences where the value of the money or property dealt with is low and the fault element consists of recklessness or negligence).

There are also time limits on prosecutions of money laundering offences at the State level. For example, in New South Wales (NSW) and Victoria there are summary offences of dealing with property suspected of being the proceeds of crime which require proceedings to be commenced no later than six and 12 months, respectively, after the offence was alleged to have been committed.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Australia has a federal system of government. There are parallel criminal offences in all Australian States and Territories that deal with the offence of money laundering. The legislation is broadly consistent across all jurisdictions and addresses the offences of dealing with the proceeds and instruments of crime. Penalties vary depending on whether the accused knew, reasonably suspected or was reckless as to the fact that they were engaged in money laundering. An exception of note is in the Australian Capital Territory where it is a strict liability offence under the *Crimes Act 1900* (ACT) to deal with property that is suspected of being the proceeds of crime. Enforcement of these laws is carried out by the relevant State or Territory police force.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Legislation at the Commonwealth, State and Territory levels in Australia enables the restraint and forfeiture of property that is an instrument of an offence or the proceeds of an offence.

Under the Commonwealth *Proceeds of Crime Act 2002* (POCA), the AFP or CDPP may apply to a court to make a restraining, forfeiture or freezing order. Restraining orders include unexplained wealth orders. The grounds for an order differ depending on the order sought. For example, on the AFP's or CDPP's application, a court must make an order that property specified in the order be forfeited to the Commonwealth if (among other grounds) a person has been convicted of one or more indictable offences and the court is satisfied that the property is the proceeds or an instrument of one or more of the offences (POCA section 48).

However, for some orders, property can be restrained and forfeited even if there has been no criminal conviction. For example, where a person is suspected of committing a serious offence, a restraining order can restrain all of the person's property (regardless of its connection to the suspected offence, POCA section 18). If such a restraining order is in force for at least six months, the AFP can apply for all the property to be forfeited to the Commonwealth, even if the suspect has not been convicted of a serious offence and the property has no connection with the offence (POCA section 47).

"*Property*" includes actual personal and real property, as well as interests in that property which are subsequently acquired (such as a mortgage). Property can be proceeds or an instrument of an offence even if the property is situated outside of Australia.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

There have been two instances where employees of a bank have been convicted of money laundering. In both instances, however, money laundering was a secondary charge. A NSW employee of the Commonwealth Bank was convicted of stealing and recklessly dealing with the proceeds of a crime after he assumed the identities of bank customers to obtain credit cards (*Butler v R* [2012] NSWCCA 54). An associate director of the National Australia Bank was convicted of insider trading and dealing with the proceeds of crime after he used confidential Australian Bureau of Statistics information to execute profitable derivatives trades (*Kamay v the Queen* [2015] VSCA 296).

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Generally criminal actions are resolved or settled through the judicial process, with imprisonment and fines being the two main outcomes. The Commonwealth, State or Territory may also apply to have the money or property of the offender seized through a forfeiture order under POCA or similar State or Territory legislation (see the response to question 1.10 above).

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Anti-money laundering and counter-terrorism financing (AML/CTF) requirements are imposed on financial institutions and other businesses under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

At a high level, the AML/CTF Act requires reporting entities (REs) to:

- enrol with AUSTRAC as an RE and (if the RE provides remittance services) apply for registration as a remittance service provider;
- undertake a money laundering and terrorism financing (ML/TF) risk assessment and monitor for ML/TF risk on an ongoing basis;
- adopt an AML/CTF Program which addresses specific matters;
- appoint an AML/CTF Compliance Officer;
- conduct employee due diligence;
- conduct due diligence (i.e. "*KYC*") and, where applicable, enhanced due diligence on customers;
- identify beneficial owners of customers and identify if the customer or beneficial owner is a politically exposed person (PEP);
- undertake transaction monitoring;
- deliver AML/CTF risk awareness training;
- report suspicious matters to AUSTRAC;
- report certain cash transactions, international funds transfer instructions and cross-border cash movements to AUSTRAC;
- report on compliance with the AML/CTF Act to AUSTRAC annually;
- ensure that components of the AML/CTF Program are subject to regular independent review; and
- pay an annual supervisory levy to AUSTRAC.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

No. RE's legal requirements are contained in the AML/CTF Act, the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules) and other regulations made under the AML/CTF Act from time to time. REs are also bound by the AML/CTF Programs they adopt, as a breach of the AML/CTF Program may also constitute a breach of one or more civil penalty provisions under the AML/CTF Act.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

No, such organisations and associations are not responsible for compliance and enforcement against their members.

2.4 Are there requirements only at national level?

Yes, there are requirements only at national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

AUSTRAC is responsible for examining REs for compliance and commencing enforcement action against REs for breaches of the AML/CTF Act.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes. AUSTRAC functions as both Australia's FIU and AML/CTF regulator.

AUSTRAC has published a monitoring policy and an information paper on its approach to regulation on its website: http://www.austrac.gov.au/about-us/policies/monitoring-policy and http://www.austrac.gov.au/businesses/obligations-and-compliance/austracs-approach-regulation.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

AUSTRAC must apply to the Federal Court for a civil penalty order no later than six years after the contravention is alleged to have occurred. There are no stipulated time limits for other enforcement actions.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum penalty for breach of a civil penalty provision under the AML/CTF Act is A$21 million per breach. Most of the key obligations under the AML/CTF Act are civil penalty provisions.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Civil and criminal actions can also be resolved through the imposition of enforceable undertakings and infringement notices. Enforceable undertakings are accepted by the AUSTRAC CEO as an alternative to civil or criminal action. An enforceable undertaking documents a binding obligation of the RE to either take a specified action or refrain from taking an action that may contravene the AML/CTF Act. The undertaking can be enforced by the courts if it is not complied with.

Infringement notices are also available for some contraventions of the AML/CTF Act. A fine usually accompanies the infringement notice. In 2018 the scope of infringement notices was expanded to allow AUSTRAC to issue infringement notices for a greater range of contraventions. An infringement notice and a A$12,600 fine for a corporation or a A$2,520 fine for an individual may be issued for contraventions against certain provisions of the Act including KYC and reporting provisions.

Remedial directions can be given by AUSTRAC to inform an entity of a specific action it must take to avoid contravening the AML/CTF Act which may include ordering an entity to undertake a ML/TF risk assessment. In 2018 the scope of remedial directions was expanded to allow AUSTRAC to issue a remedial direction to an RE directing it to remedy a breach of a reporting provision by submitting reports to AUSTRAC within a specified timeframe. A breach of a remedial direction is a breach of a civil penalty provision (unless the RE is a remittance service provider or digital currency exchange provider in which case it may be a criminal offence).

AUSTRAC also has the power to suspend or cancel a remittance provider's registration or a digital currency exchange provider's registration if they have contravened the AML/CTF Act or present a significant ML/TF risk, people smuggling risk (in respect of remittance) or other serious crime risk.

There is no specific liability regime under the AML/CTF Act applicable to directors, officers and employees. However, such individuals may be liable for an ancillary contravention of a civil penalty provision if they aid, abet, counsel, procure, induce, are knowingly concerned in or party to, or conspire with others to effect a contravention of a civil penalty provision of the AML/CTF Act. Further, directors have obligations under the *Corporations Act 2001* which may be breached if a company does not comply with its obligations under the AML/CTF Act.

There are no general powers under the AML/CTF Act to suspend or bar individuals from employment in certain sectors, although the AUSTRAC CEO may cancel a person's registration as a remittance service provider.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Most of the penalties under the AML/CTF Act are civil in nature. This means that the sanctions are not imposed through the criminal process and accordingly only require the civil standard of proof (the balance of probabilities) to attract a penalty. These sanctions include monetary fines, enforceable undertakings and infringement notices.

Some breaches will attract criminal sanctions, including the tipping off prohibition (see the response to question 3.8 below). It is also a criminal offence to provide, possess or make a false document, operate a designated service under a false name, or conduct cash transactions with the aim of avoiding reporting requirements. Operating an unregistered remittance business or unregistered digital currency exchange business will also attract criminal sanctions.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

AUSTRAC has investigative powers to compel entities to produce documents. It will generally use these powers to conduct reviews of REs on a regular basis. The fact that AUSTRAC is conducting a review of an entity or the results of those reviews are not made public unless it proceeds to a formal sanction.

If AUSTRAC wishes to pursue a civil penalty or an injunction, AUSTRAC's CEO must apply to the Federal Court for an order to that effect. The application for an order, any defence filed and the court's decision are all publicly available.

Infringement notices may be given by an authorised officer and copies are available on AUSTRAC's website. Remedial directions and enforceable undertakings may only be issued by the AUSTRAC CEO and are available on AUSTRAC's website. Remedial directions and enforced external audits are reviewable outside the court system. If the decision is made by an AUSTRAC delegate, it may be reviewed by the AUSTRAC CEO whose decision may in turn be reviewed by the Administrative Appeals Tribunal.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The AML/CTF Act applies to designated services provided at or through a permanent establishment in Australia or, if the provider has a certain Australian connection, provided at or through a permanent establishment outside Australia.

There are at least 70 designated services, grouped into financial services, bullion dealing and gambling services. If the person provides a designated service with the requisite geographical link, the person is an RE and must comply with the AML/CTF Act (see the response to question 2.1 above).

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

On 3 April 2018 the AML/CTF Act was amended to include a new designated service which may apply to cryptocurrency products. Persons who exchange digital currency for money (whether Australian or not), or exchange money (whether Australian or not) for digital currency, where the exchange is provided in the course of carrying on a digital currency exchange business, are REs and must comply with the AML/CTF Act. Providers of this designated service must also register on the Digital Currency Exchange Register maintained by AUSTRAC.

"*Digital currency*" is defined in the AML/CTF Act as a digital representation of value that functions a medium of exchange, store of economic value or unit of account which is not issued by or under the authority of a government body. The representation of value must be interchangeable with money, may be used as consideration for the supply of goods or services and is generally available to members of the public without any restriction on its use as consideration. A means of exchange or digital process or crediting may also be declared to be digital currency by the AML/CTF Rules.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes. The AML/CTF Program generally must be composed of a Part A and a Part B and specifically address matters prescribed by the AML/CTF Act and AML/CTF Rules. These matters generally align with the obligations under the AML/CTF Act outlined in the response to question 2.1 above.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

If an RE commences to provide, or provides a designated service to a customer and the provision of the service involves a transaction involving the transfer of A$10,000 or more in physical currency, the RE must report the transaction to AUSTRAC within 10 business days after the day on which the transaction took place.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Yes. REs must report suspicious matters to AUSTRAC (see the response to question 3.8 below). There is an obligation on banks and remittance providers to report international funds transfer instructions (IFTIs) to AUSTRAC. The obligation applies to the last person to send the IFTI out of Australia (for outgoing instructions) and the first person to receive the IFTI from outside Australia (for incoming instructions). There are no dollar thresholds applicable to suspicious matter or IFTI reporting.

A person moving physical currency of A$10,000 or more into or out of Australia must report the movement to AUSTRAC, a customs officer or a police officer.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

See the response to question 3.5 above.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Before providing a designated service to a customer, the RE must undertake the applicable customer identification procedure set out in Part B of its AML/CTF Program. The procedure to be undertaken will depend on the type of customer being onboarded. The AML/CTF Rules require Part B to contain specific procedures for customers who are individuals, companies and trustees (among other types of entities). Generally, the process requires collection of prescribed information and verification of that information from reliable and independent documents or electronic data.

REs are required to conduct enhanced due diligence on the customer if (in addition to any other trigger events set out in the RE's AML/CTF Program):

- the RE determines under its risk-based systems and controls that the ML/TF risk is high;
- a designated service is being provided to a customer who is or who has a beneficial owner who is a foreign PEP;
- a reportable suspicion has arisen; or
- the RE is entering into or proposing to enter into a transaction with a party physically present in (or is a corporate incorporated in) a prescribed foreign country, which currently includes the Democratic People's Republic of Korea and Iran.

REs must also conduct ongoing customer due diligence in accordance with the AML/CTF Rules and their AML/CTF Program.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes. A financial institution must not enter into a banking relationship with a shell bank or a banking institution that has a banking relationship with a shell bank. If a bank subsequently finds out that it is in a shell bank arrangement, it must terminate the relationship within 20 business days. The definition of shell bank in the AML/CTF Act covers financial institutions and affiliates which have no physical presence in the country they are incorporated in.

3.9 What is the criteria for reporting suspicious activity?

At a high level, an RE has a suspicious matter reporting obligation if:

- the RE commences to provide or proposes to provide a designated service to a person, or a person requests the RE to provide them with a designated service or inquires whether the RE would be willing or prepared to provide them with a designated service; and
- the RE suspects on reasonable grounds that:
  - the person (or their agent) is not who they claim to be;
  - the provision or prospective provision of the designated service is preparatory to the commission of a money laundering or terrorism financing offence;
  - the RE has information that may be relevant to the investigation of or prosecution of a person for a money laundering offence, for a terrorism financing offence, for evasion or attempted evasion of a tax law, or for **any other offence** against a law of the Commonwealth or of a State or Territory; or
  - the RE has information that may be of assistance in the enforcement of proceeds of crime laws.

If a suspicious matter reporting obligation has arisen, the RE must not disclose to someone other than AUSTRAC:

- that the RE has reported a suspicion to AUSTRAC;
- that the RE has formed a reportable suspicion; or
- any other information from which the recipient of the information could reasonably be expected to infer that the report has been made or that the suspicion has been formed.

There are some exceptions to the tipping off prohibition, including certain disclosures to law enforcement bodies, legal practitioners and other members of a RE's designated business group.

Suspicious matter reporting does not constitute a legal safe harbour or defence to prosecution of the RE for a criminal offence (including money laundering offences).

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The Australian Securities and Investments Commission (ASIC) maintains information about each Australian company's directors,

shareholders and ultimate holding company. ASIC does not maintain information about the natural persons who are the entities' ultimate beneficial owners. This means that the register does not assist in compliance with beneficial ownership requirements.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Banks who accept a transfer instruction at or through a permanent establishment of the bank in Australia must obtain certain information about the payer and, before passing on the transfer instruction to another person in the funds transfer chain, ensure that the instruction includes certain information about the payer.

Interposed institutions in the funds transfer chain must also pass on certain information about the payer.

Certain information about the payer and payee must be included in reports to AUSTRAC of IFTIs transmitted out of Australia.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The *Corporations Act 2001* prohibits an Australian-registered company from issuing bearer shares. Bearer shares are still permitted if a company has transferred its registration to Australia from a jurisdiction where bearer shares are legal. In this instance, a bearer shareholder has the option of surrendering the bearer share. If they do so, the company must cancel the bearer share and include the bearer's name on their register of members.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes. See the response to question 3.1 above. There is also a proposal to extend the AML/CTF Act to other areas including lawyers, accountants and real estate agents.

Further, the predecessor to the AML/CTF Act, the *Financial Transaction Reports Act 1988* (FTR Act) is still in force for some businesses. The FTR Act imposes reporting requirements on "*cash dealers*" to report suspicious transactions and verify the identity of persons who are account signatories. Solicitors are also required under the FTR Act to report any cash transactions over A$10,000 (or the foreign currency equivalent).

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No. AML/CTF requirements are generally applicable in respect of customers who are receiving designated services from the RE.

Some obligations may only apply where a person has a connection to a prescribed foreign country, which currently includes the Democratic People's Republic of Korea and Iran.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

A statutory review of the AML/CTF Act was undertaken by the Commonwealth Attorney-General's Department in 2013 to 2016 which resulted in 84 recommendations in relation to Australia's AML/CTF regime. The government is in the process of implementing the recommendations in phases. The first phase, which has been implemented, addresses the regulation of digital currency exchange providers, AUSTRAC's power to issue infringement notices and some deregulatory measures.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In 2015, FATF identified deficiencies in Australia's compliance with the FATF recommendations. FATF's key findings include that Australia should:

- focus more on identifying ML/TF risks, with a particular emphasis on the not-for-profit sector;
- substantially improve the mechanisms for ascertaining and recording beneficial owners in the context of customer due diligence, especially in the context of trustee information retention;
- take a more active role in investigating and prosecuting money laundering offences; and
- extend the AML/CTF regime to Designated Non-Financial Businesses and Professions, including lawyers, real estate agents and accountants.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes. FATF evaluated Australia's AML/CTF regime in 2014 to 2015, releasing its report in April 2015. The report is available on FATF's website http://www.fatf-gafi.org/documents/documents/mer-australia-2015.html.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The AML/CTF Act and related legislation are published on the website https://www.legislation.gov.au/. AUSTRAC publishes guidance on its website http://www.austrac.gov.au/.

Kate Jackson-Maynes

King & Wood Mallesons
Level 61, Governor Phillip Tower
1 Farrer Place
Sydney NSW 2000
Australia

Tel: *+61 2 9296 2358*
Email: *kate.jackson-maynes@au.kwm.com*
URL: *www.kwm.com*

Kate is a Partner in the Banking and Finance team of King & Wood Mallesons.

Kate specialises in anti-money laundering, counter-terrorism financing, proceeds of crime and sanctions and the ground-breaking areas of blockchain and regtech. In her role, Kate advises banks and other financial institutions, payment services providers, casinos and gaming companies and fintechs in Australia and offshore on complying with the Australian regime and the expectations of the regulator AUSTRAC. Kate and her team have also created bespoke regtech tools for their clients to assist with compliance with AML/CTF and sanctions laws.

Kate also specialises in other financial services regulation including Australian financial services and credit licences and privacy.

In recognition of her achievements, Kate is a ranked lawyer for Financial Services Regulation in the 2019 *Chambers and Partners Asia-Pacific Guide* and was listed as one of Australia's Best Lawyers from 2015 to 2018 in the Banking and Finance division.

Amelia Jamieson

King & Wood Mallesons
Level 61, Governor Phillip Tower
1 Farrer Place
Sydney NSW 2000
Australia

Tel: *+61 2 9296 2208*
Email: *amelia.jamieson@au.kwm.com*
URL: *www.kwm.com*

Amelia is a Senior Associate in King & Wood Mallesons' financial services regulation team, specialising in anti-money laundering and counter-terrorism financing, financial services licensing and payments.

Amelia works with Australian banks, global financial institutions and fintechs, advising on market entry, product design, licensing and regulatory compliance. Complementing her regulatory expertise, Amelia has also designed a number of AML/CTF regtech tools for clients, which streamline and automate KYC, risk assessments and IFTI reporting.

Amelia works regularly with clients to help design and implement their AML/CTF Programs, ensuring they comply with the AML/CTF Rules and address the money laundering and terrorism financing risks the clients face.

Before joining King & Wood Mallesons, Amelia worked in the Royal Bank of Canada's global AML policy team in the bank's Toronto headquarters.

KING&WOOD
MALLESONS
金杜律师事务所

Recognised as one of the world's most innovative law firms, King & Wood Mallesons offers a different perspective to commercial thinking and the client experience. With access to a global platform, a team of over 2,000 lawyers in 27 locations around the world works with clients to help them understand local challenges, navigate through regional complexity, and to find commercial solutions that deliver a competitive advantage for our clients.

As a leading international law firm headquartered in Asia, we help clients to open doors and unlock opportunities as they look to Asian markets to unleash their full potential. Combining an unrivalled depth of expertise and breadth of relationships in our core markets, we are connecting Asia to the world, and the world to Asia.

Always pushing the boundaries of what can be achieved, we are reshaping the legal market and challenging our clients to think differently about what a law firm can be.

Austria

Wolf Theiss Rechtsanwälte GmbH & Co KG

Markus Heidinger

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In general, money laundering is prosecuted on a regional level by the respective public prosecutor's office. Though, the prosecution is concentrated with the public prosecutor's office for business crime and corruption (*Wirtschafts- und Korruptionsstaatsanwaltschaft*) in Vienna for specific cases where the money or other assets are the proceeds of specific predicate offences (section 20a of the Austrian Criminal Procedure Code (*StPO*).

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Section 165 para 1 of the Austrian Criminal Code (*StGB*) defines money laundering by the following elements: (1) money or other assets are the proceeds of a predicate offence; (2) the proceeds are intentionally concealed or the origin disguised; and (3) the offender is aware that the money or other assets are proceeds stemming from a predicate offence and acts with intent in this respect.

In addition, section 165 para 2 *StGB* defines as criminal money laundering the acceptance, keeping in custody, investment, administration, conversion, realisation or transfer of proceeds of a predicate offence, if the offender knows that the proceeds result from a predicate offence.

Last but not least section 165 para 3 *StGB* defines as money laundering such cases, where the offender knowingly accepts, takes into custody, invests, administers, converts, realises or transfers to a third person money or other assets which is under the control of a criminal organisation or a terrorist organisation upon instruction of or in the interest of such criminal organisation or terrorist organisation, respectively.

Predicate offences for the purposes of money laundering are (§ 165 para 1 *StGB*):

- all crimes with a potential sentence of more than one year of imprisonment; and
- some specific crimes with lower potential sentence explicitly mentioned (for instance, document forgery, suppression of documents, giving false evidence in court or towards administrative authorities).

Tax evasion may, depending on the circumstances and the amounts, be punishable under the Austrian Financial Crime Code, and may qualify as a predicate offence as well, provided that the specific case is punishable with a maximum of more than one year of imprisonment. However, the criterion "money or assets are the proceeds of a predicate offence" might not be fulfilled for mere tax savings.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In general, Austrian criminal law is applicable if the crime is committed in Austria (section 62 *StGB*) or on an aircraft/ship operating under the Austrian flag (section 63 *StGB*).

Further, Austrian criminal law applies irrespective of the criminal law of the place of the crime for the intentional participation in a criminal offence which the direct offender has committed in Austria, and Austrian criminal law will apply to money laundering with respect to a predicate offence committed in Austria (§ 64 para 1 number 8 *StGB*). In other cases, Austrian Criminal Law will apply to money laundering committed outside of Austria provided that at the time of the offence the laws of the place of the offence do also make money laundering a criminal offence and the offender at the time of the offence was an Austrian national or, if Austrian nationality was acquired at a later time, the offender still was an Austrian national at the time of the initiation of the criminal proceedings. Similarly, an offender who at the time of the offence was a non-citizen may be punished in Austria if he is caught in Austria and can for certain reasons not be extradited.

Proceeds from a foreign crime will qualify as proceeds from a predicate offence under section 165 STGB, if the crime was punishable at the place of the crime and the predicate offence is comparable to a predicate offence in Austria.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The competent authority for the prosecution of money laundering criminal offences is the locally competent public prosecutor's office. For certain cases it is the public prosecutor's office for business crime and corruption (see question 1.1 above). Investigations will be conducted by the regional police office upon instruction of the public prosecutor's office, if upon instruction of the public prosecutor's office for business crime and corruption

investigations will typically be conducted by the Federal Office for the Prevention of and Combat against Corruption (*Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung*).

1.5 Is there corporate criminal liability or only liability for natural persons?

The Austrian Criminal Code (*StGB*) contains the provisions for the criminal liability of natural persons. In addition, Austria has in 2005 introduced an act on corporate criminal liability (*Verbandsverant wortlichkeitsgesetz*) and corporates and financial institutions may be subject to criminal liability for money laundering under the conditions laid down in this act as well.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

In case the proceeds from the predicate offence exceed the value of EUR 50,000 or in case money laundering is committed as a member of a criminal organisation established for continuous money laundering, the maximum sentence is up to 10 years' imprisonment. In other cases, the maximum sentence is up to three years' imprisonment. The maximum penalty for corporates is EUR 1,300,000 in cases where the maximum sentence for natural persons is up to 10 years, and EUR 850,000 in cases where the maximum sentence for natural persons is three years.

1.7 What is the statute of limitations for money laundering crimes?

There is no specific limitation period for money laundering crimes but the general limitation periods for crimes apply. The limitation period for crimes with a maximum sentence of three years' imprisonment is five years; the limitation period for crimes which are punishable with imprisonment of up to 10 years is 10 years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

The exclusive competence is at the national level, no parallel state or provincial criminal offences exist.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Section 19a *StGB* regulates the confiscation of objects which the offender has used for the offence or which have been brought about by the offence, including substitute assets to which the offender holds property at the time of the criminal court decision of first instance. Forfeiture is regulated by section 20 *StGB* and applies to all money/assets obtained by the offender for the commitment of a crime or by committing a crime. It extends to the use of such assets as well as to substitute assets. In case of money laundering, section 20b *StGB* facilitates forfeiture insofar as it can be extended to all assets acquired in a time context with the money laundering in case there is reason for suspicion that they result from an illegal act.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Banks, other regulated financial institutions and their directors have been subjected to administrative penalties for non-compliance with regulations on the prevention of money laundering. When it comes to criminal proceedings, publicly available information is limited insofar as proceedings may be resolved without public prosecution and public hearings. From public records, no bank or other regulated financial institution has been convicted of money laundering under corporate criminal responsibility so far.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The only way to resolve criminal actions is through the judicial process. There is no formal settlement. What exists is a so-called *Diversion*. The facts and terms of a *Diversion* are not public. Court hearings are of course public, but decisions of the lower courts are not published and decisions of the Supreme Court are published only on a no-name basis.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The supervising authorities for compliance with anti-money laundering regulations are:

- for banks and other financial institutions, the Financial Market Authority ("*FMA*");
- for lawyers in private practice, the regional bar association;
- for notaries, the national chamber of notaries;
- for auditors and tax advisors, the federal chamber of auditors and tax advisors;
- for certified accountants, the federal chamber of commerce;
- for gaming companies and casinos, the federal ministry of finance; and
- for companies, trading with goods the local trade authority.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Lawyers, notaries, auditors and tax advisors, and certified accountants are regulated by self-regulatory bodies. These might impose binding anti-money laundering requirements on a secondary level.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, for self-regulated professions like lawyers, notaries, and auditors and tax advisors, the relevant self-regulatory professional organisation is responsible for anti-money laundering compliance

and enforcement against their members. For lawyers, this is the regional Bar association, for notaries, the national chamber of notaries, for auditors and tax advisors, this is the federal chamber of auditors and tax advisors, and for certified accountants, it is the federal chamber of commerce.

2.4 Are there requirements only at national level?

Yes, the anti-money laundering requirements are codified in federal acts; the core act is the Financial Market Money Laundering Act (*Finanzmarkt-Geldwäschegesetz*) which codifies the anti-money laundering requirements for the financial industry.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

For the financial industry, the competent authority is the *FMA*. The *FMA* has published a number of circular letters:

- circular letter 08/2011 regarding the notification of suspicious transactions;
- circular letter 03/2018 regarding risk analysis on the prevention of money laundering and terrorist financing;
- circular letter 09/2018 on duties of care for the prevention of money laundering and terrorist financing; and
- circular letter 01/2019 regarding notification obligations for the prevention of money laundering and terrorist financing is in consultation and likely to be published by May 2019.

All circulars of the *FMA* are available on the website www.fma.gv.at.

Self-regulatory bodies like the Bar associations, the chamber of auditors and tax advisors, or the chamber of notaries have published guidelines for their members; the guidelines are usually for members only and are not usually publicly available.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the Austrian FIU is the Money Laundering Notification Office (*Geldwäschemeldestelle*), which is located at the Federal Ministry of the Interior.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

In the core act, the Financial Market Money Laundering Act, the statute of limitation is three years for penalties for breach of anti-money laundering regulations. For other regulatory actions under the financial money laundering act, no specific limitation period exists. Limitation statutes in other relevant acts (for lawyers, auditors, etc.) differ slightly.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Regarding the financial industry, governed by the Financial Market Money Laundering Act, almost all violations of duties under this act are subject to penalty provisions. In case of particularly grave and systematic violations, the maximum administrative penalty for natural persons is EUR 5,000,000 or the double of the benefit obtained by the violation. For legal entities, the maximum corporate penalty is EUR 5,000,000 or 10% of the cross income of the entity in the preceding year, depending on which figure is higher.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The *FMA* as the competent authority for financial institutions may order specific compliance measures, it may declare directors to be not fit and proper anymore and demand the dismissal of directors by the regulated entity. In repeated severe cases it may even revoke the licence of a regulated entity.

Types of sanctions for other industries and professions subject to anti-money laundering regulations differ but are usually less severe than under the Financial Market Money Laundering Act.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

The penalties are of an administrative nature.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

In case of suspicion that anti-money laundering regulations have been violated, the competent authority will initiate an investigation. If the regulated entity and/or the responsible persons are found guilty of a violation, the competent authority will issue a decision on the penalty. Decisions of penalty actions by the competent authority are usually not public; only in the financial industry the FMA will usually publish the fact that it has rendered a decision, but not the decision itself. Penalised persons and institutions can appeal against the penalty decision. The appeal for financial institutions and its directors for penalties under the Financial Market Money Laundering Act is decided by the Federal Administrative Court (*Bundesverwaltungsgericht*), and financial institutions and their directors have in the past quite often challenged penalty assessments by the *FMA*, but in most cases unsuccessfully.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The Financial Market Money Laundering Act applies to credit institutions and financial institutions. Financial institutions include insurance undertakings within the scope of their life assurance operations, investment firms and investment services providers, alternative investment fund managers, e-money institutions, payment institutions, and Austrian branches of certain member state financial institutions.

Other businesses which are subject to anti-money laundering requirements include certain professions like lawyers, notaries, auditors and tax advisors, real estate brokers, gambling companies and companies trading with certain commercial goods.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

For the time being, anti-money laundering requirements have applied to the cryptocurrency industry only in cases where a player in the industry required a licence for some financial services business (for instance, MIFID or payment services). An explicit inclusion of the cryptocurrency industry will be achieved by the implementation of the 5th Anti-Money Laundering Directive of the EU.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All obliged entities (financial industry, lawyers, etc.) are required to maintain compliance programmes which include risk management, application of due diligence, reporting and recordkeeping obligations are met and regularly monitored, and suspicious activity reports are properly filed.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Proper recordkeeping is part of the customer on-boarding process. Reporting obligations exist with regard to suspicious activities, i.e. when an obliged entity has reason for the suspicion that a transaction or an activity relates to proceeds from a predicate offence.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There are no such routine report requirements under anti-money laundering regulations.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There are no such reporting requirements under anti-money laundering regulations. Though, certain reporting requirements exist under tax laws and for statistical purposes.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

General customer identification and due diligence requirements include the identification of the client, the identification of the ultimate beneficial owner, and analysis on the money laundering risk. When assessing the customer-related risk the obliged entity has to consider the purpose of the business relationship, the amount of the assets, the regularity, and duration of the business relationship.

Enhanced due diligence requirements exist for politically exposed persons, customers from high-risk jurisdictions and in the case that the risk analysis shows a high-risk (taking into account the risk indicators of the annexes to the Financial Market Money Laundering Act), which reflect the annexes of the 4th Anti-Money Laundering Directive.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Shell banks need to be treated as high-risk customers.

3.9 What is the criteria for reporting suspicious activity?

A suspicious activity report has to be filed if the facts indicate ("give reason to suspect") that money/assets are connected to the business relationship, a specific transaction or a brokerage related to a crime which is a predicate offence to money laundering or to terrorist financing, or if there are indications that the client has failed to correctly disclose beneficial ownership.

Lawyers and other professionals might be exempt from suspicious activity reporting if the respective circumstances are covered by their professional privilege.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

All companies including partnerships with legal capacity have to be registered with the Austrian commercial register which is publicly accessible and typically contains information on the management and for limited liability companies and partnerships also information on shareholders/partners. In 2018, Austria established a "Beneficial Owner Register" where all Austrian legal entities have to disclose information on their beneficial ownership. Access to the beneficial ownership register is not public, though financial institutions and other obliged entities have access for the purpose of compliance with their AML customer due diligence responsibility.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Payment orders need to contain sufficient information on the originator and an account number through which the transfer is made. Standard payment orders include the name of the recipient, but the bank is not required to check whether this name matches the account number.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Only for stock corporations whose shares are listed at an exchange.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Specific anti-money laundering regulations apply to various professions and to various businesses trading in goods.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Anti-money laundering requirements apply to persons trading with certain commercial goods (see question 3.1 above). No specific anti-money laundering requirements exist for free trade zones.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Currently, the implementation of the 5th Anti-Money Laundering Directive of the EU is being prepared. Ongoing initiatives regarding international information exchange in the area of taxation may at least in part also be seen as anti-money laundering measures.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In reaction to a rather critical report by the FATF in 2015/2016, the Austrian government has significantly increased its efforts in the area of prevention of and combat against money laundering and terrorist financing. The follow-up report of the FATF in December 2017 is available on the website of the FATF, and a number of FATF recommendations have been re-rated.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

In September 2016, the FATF published its mutual evaluation report on Austria. Following this, Austria is now in an enhanced follow-up process and the first follow-up report was published in December 2017.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

All Austrian national laws and regulations are available online on the national legal information system www.ris.bka.gv.at. An English translation of the "Beneficial Owners Register Act" and of the "Financial Markets Money Laundering Act" is available on the website of the Austrian Financial Market Authority www.fma.gv.at/en/national/supervisory-laws/#58.

Markus Heidinger

Wolf Theiss Rechtsanwälte GmbH & Co KG
Schubertring 6
1010 Vienna
Austria

Tel: *+43 1 51510 5060*
Email: *markus.heidinger@wolftheiss.com*
URL: *www.wolftheiss.com*

Markus Heidinger is a member of the Banking & Finance team. He specialises in banking law, financial institutions and markets, corporate and corporate finance law, including dispute resolution and regulatory investigations and proceedings in those areas. He is an internationally recognised banking and financial markets regulatory, funds and corporate finance expert who also has substantial experience in all sorts of financing litigation and transactions, corporate finance structures and corporate transactions in the financial industry. Highly renowned in the market, Markus is ranked in band 1 for Banking and Finance in *Chambers* (2018) as well as a Leading Individual for Banking and Finance in *The Legal 500* (2018). He is also a recommended by *The Legal 500* (2018) for Capital Markets. He has been the Austrian correspondent of the *Journal of International Banking Law and Regulation* since the 1990's and served as a panel member of the Vienna Bar Association from 2008 to 2015.

WOLF THEISS

Since starting out in Vienna some 60 years ago, we have grown into one of the largest and leading commercial law firms in Central, Eastern and South-Eastern Europe (CEE/SEE). We now employ 340 lawyers, working across numerous practice areas in 13 countries including Albania, Austria, Bosnia and Herzegovina, Bulgaria, Croatia, the Czech Republic, Hungary, Poland, Romania, Serbia, the Slovak Republic, Slovenia and Ukraine. Apart from our local-offices, we use a well-established network of contacts with well-respected local lawyers and other service providers to advise and assist our clients in other countries in the region, such as Kosovo, Moldova, Montenegro, North Macedonia and Turkey.

Wolf Theiss is one of the very few law firms with long-standing well-established practice in compliance, AML and other law related practices, with a strong focus and expertise in the banking & finance sector.

Belgium

Françoise Lefèvre

Rinaldo Saporito

Linklaters LLP

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering is an offence prosecuted by the office of the public prosecutor or by an investigating judge and tried before the Belgian criminal courts.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

For the criminal offence of money laundering to be established, the prosecution must prove that some specific actions have been carried out by the agent (*actus reus*) with a certain intention (*mens rea*). More particularly, money laundering refers to three distinct criminal behaviours:

- **Article 505, 1st indent, 2°, of the Belgian Criminal Code (hereafter, the "BCC")**, incriminates the acts of buying, receiving, exchanging, possessing, keeping or managing assets derived from a predicate offence, but only if the agent knew or ought to have known, at the outset of each operation, that the assets derived from an illicit origin.

  A third party (i.e. a person who is not the owner of the illicit assets) can also be prosecuted on the grounds of this provision, unless the illicit assets are derived from a "simple" tax fraud.

  Case law outlines that the author of the predicate offence may not be prosecuted on the grounds of this provision unless the said predicate offence has been carried out abroad and may not be prosecuted in Belgium.
- **Article 505, 1st indent, 3°, BCC**, incriminates the acts of converting or transferring assets derived from a predicate offence. *Mens rea* is in this case more specific than under article 505, 1st indent, 2°, BCC: there must be evidence that the agent acted with the intent to conceal the illicit origin of the funds or to help any person involved in the predicate offence to avoid the legal consequences of his/her acts.

  Both the agent that has committed the predicate offence and a third party can be prosecuted on the grounds of this provision.
- **Article 505, 1st indent, 4°, BCC**, incriminates the acts of concealing or disguising the nature, the origin, the location, the disposition, the movements or the ownership of the assets derived from a predicate offence. The conduct referred to in this provision is particularly extensive, so much so that it overlaps with most of the acts incriminated under the other branches of article 505 BCC. *Mens rea* is understood as broadly as under article 505, 1st indent, 2°, BCC: the agent may be prosecuted only if he/she knew or ought to have known that the assets derived from an illicit origin.

  Both the agent that has committed the predicate offence and a third party can be prosecuted on the grounds of this provision. However, and as under article 505, 1st indent, 2°, BCC, the latter may not be prosecuted if the illicit assets derive from a "simple" tax fraud.

Every offence referred to in the Belgian Criminal Code or in another law that can generate assets (such as illicit tax evasion) can be a predicate offence to money laundering.

It is not necessary for the prosecution to precisely identify the predicate offence as long as it has been demonstrated that the assets have an illicit origin (for instance, because the accused person gave no plausible explanation of the origin of the funds).

The fact that the predicate offence can no longer be prosecuted because the limitation period has expired is not an obstacle for the Belgian authorities to prosecute money laundering behaviours on the funds derived from the time-barred offence.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The predicate offence does not have to fall within the territorial jurisdiction of Belgian courts for money laundering itself to be validly prosecuted in Belgium, provided that the predicate offence is incriminated both in Belgium and in the foreign country where the predicate offence was carried out. Money laundering itself can be prosecuted in Belgium even if it has been partially committed in a foreign country, provided that some of the acts have been carried out in Belgium.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

See question 1.1.

1.5 Is there corporate criminal liability or only liability for natural persons?

Both legal entities and natural persons can be held liable for the offence of money laundering.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The individual found guilty of money laundering can be sentenced to a maximum term of imprisonment of five years and/or to pay a fine of maximum €800,000. Companies can be sentenced to pay a maximum fine of €1,600,000.

1.7 What is the statute of limitations for money laundering crimes?

The limitation period for money laundering is five years. However, the repetition of criminal acts carried out with the same intention could delay the starting point of the five-year limitation period to the date of the last act that was executed by the agent.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes, enforcement is only at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Confiscation is mandatory for all the assets on which one of the prohibited acts referred to in article 505, 1st indent, 2° to 4°, BCC, has been carried out, as well as on the proceeds derived from them, even if they do not belong to the convicted person. The confiscation will be ordered by the judge as a consequence of a conviction for money laundering, to the profit of the Belgian State. There is no non-criminal confiscation, nor civil forfeiture.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, this has happened.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions can be settled with the public prosecutor on the grounds of article 216*bis* of the Code of criminal procedure, provided that the considered offence does not entail a sentence of more than two years of imprisonment and does not involve serious harm to physical integrity.

Suspects can also enter into a guilty plea with the prosecution on the grounds of article 216 of the Code of criminal procedure. The criminal court can only approve or reject the plea agreement, without any possibility to amend the sanctions proposed by the public prosecutor. Grounds for refusing to approve the agreement are essentially threefold: (i) the agreement will be rejected if it has been demonstrated that the suspect's consent to enter the agreement was not free and informed; (ii) if the agreement does not correspond to the reality of the facts and to their legal characterisation; or (iii) if the sanctions proposed by the prosecution are not proportionate to the facts of the case at hand, to the personality of the defendant and to his/her willingness to compensate for the damage caused. These settlements are not public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

There are various authorities whose competence depends on the obliged entity.

Competent Authority	Obliged Entity
Minister of Finance	National Belgian Bank
Treasury administration	The Public Trustee Office (*Caisse des dépôts et consignations / Deposito- en Consignatiekas*); the limited company under public law Bpost
National Belgian Bank (NBB)	Credit institutions, insurance companies, payment institutions, electronic money issuers, clearing institutions, mutual guarantee societies and stock exchange firms
Financial Services and Markets Authority (FSMA)	Investment firms authorised under Belgian law in their capacity of asset management and investment advice companies; management companies of undertakings for collective investment; management companies of alternative undertakings for collective investment; investment firms provided that and to the extent that these firms trade their securities themselves; debt investment firms provided that and to the extent that these firms trade their securities themselves; alternative funding platforms; market operators; persons established in Belgium who, by way of their business activity, carry out sales of foreign currency in the form of cash or cheques expressed in foreign currencies, or by using a credit or payment card; intermediaries in banking and investment services; independent financial planners; insurance intermediaries that exercise their professional activities without any exclusive agency contract in one or more of the classes of life insurance; and lenders that are engaged in consumer credit or mortgage credit activities
Ministry of Economy, SMEs, Middle Class and energy	Companies engaged in lease financing, company service providers, diamond traders and real estate agents

Competent Authority	Obliged Entity
Auditors' Supervisory Board	Corporate auditors
Institute of Accountants and Tax Consultants	Accountants and Tax Consultants
Professional Institute of Chartered Accountants and Tax Consultants	Chartered Accountants and Tax Consultants
National Chamber of Notaries	Notaries
National Chamber of Bailiffs	Bailiffs
The Head of the Bar	Lawyers (under the conditions mentioned in Article 5 § 1 28°)
Ministry of Internal Affairs	Private security companies
Commission for Gambling Activities	Natural or legal persons active in the gambling sector

Notwithstanding the criminal and administrative sanctions that can be imposed by the competent authorities (see question 2.8 below), the latter can compel the obliged entities (i) to respect the provisions of the 18 September 2017 Act on the Prevention of Money Laundering and Terrorist Financing (hereinafter, "**the 18 September 2017 Act**"), (ii) to amend their internal organisation, and (iii) to replace their compliance officer and the person within the Board of Directors that is responsible for the implementation, in the company, of the obligations set out by the 18 September 2017 Act.

In the event the obliged entity does not comply with such injunction, the competent authority can:

- make public the offences committed by the obliged entity;
- impose a daily maximum penalty of €50,000;
- compel the obliged entity to replace its Board of Directors;
- suspend or prohibit all or part of the obliged entity's activities; and
- revoke its licence (article 91 *et seq.*).

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes, some self-regulatory organisations such as the Bar, the Chamber of Notaries or the Chamber of Bailiffs (see question 2.1 above) are responsible for anti-money laundering compliance and enforcement against their members. For example, they essentially ensure that their members respect their obligations of customer due diligence and that they report any suspicious transactions.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, see questions 2.1 and 2.2 above.

2.4 Are there requirements only at national level?

No. For instance, the local divisions of the Bar, of the Chamber of Notaries, of the Chamber of Bailiffs, etc. are responsible for enforcement against their members.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

See question 2.1 above for the competent authorities. The examination criteria are set out by the 18 September Act 2017, which is publicly available.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the CTIF (*Cellule de traitement des informations financières*) is responsible for this.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitations for administrative sanctions.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

It varies depending on the regulation concerned. For example, if they do not comply with the obligations set out in the 18 September 2017 Act, legal entities can be fined with a maximum penalty of 10% of the net annual turnover of the previous financial year and natural persons with a maximum penalty of €5,000,000 (article 132).

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

It varies depending on the regulation concerned. Within the legal framework set out by the 18 September 2017 Act, notwithstanding the sanctions that can be taken by the competent authorities in case the obliged entities do not comply with their injunctions (see question 2.1 above), the Act compels the competent authorities to publish the name of the obliged entity that has been sanctioned and the sanctions that were imposed (article 135).

The Act also foresees a term of imprisonment of a maximum of one year and/or a maximum fine of €2,500,000 for those who impede inspections by the authorities in Belgium or abroad, or who refuse to provide information that they are required to give or if they knowingly give inaccurate or incomplete information (article 136).

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, penalties are not only administrative/civil. Yes, violations of anti-money laundering obligations are subject to criminal sanctions. See questions 2.8 and 2.9 above.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

It is the Brussels Court of Appeal that is competent for the appeals against the sanctions imposed by the NBB and the FSMA.

a) No, they are not.

b) Yes, they have.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

All the obliged entities listed in the table under question 2.1 and their branches which are established in Belgium (hereinafter, the "obliged entities") are subject to the 18 September 2017 Act. This law imposes four main obligations on the obliged entities:

- Development of internal policies, controls and procedures (articles 8 to 15).
- Risk assessment (articles 16 to 18).
- Customer and operations due diligence (articles 19 to 44).
- Analysis of atypical transactions and reporting obligations (articles 45 to 65).

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Anti-money laundering requirements do not yet exist in Belgium for the cryptocurrency industry. Belgium is, however, expected to implement the 5th AML Directive by 10 January 2020, which compels Member States to designate virtual currency exchange platforms as obliged entities.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

The obliged entities are compelled to implement a compliance programme at the level of the "group", which is a compliance programme also applied at the level of the entity's subsidiaries and branches irrespective of their location. In other terms, the obliged entities' subsidiaries and branches must apply all the obligations set out by the 18 September 2017 Act, even if they are located in another EEE Member State or in a third country (article 13).

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

The obliged entities must keep a copy of all the documents and evidence necessary to identify their clients for a period of 10 years, which starts from the date of the end of the business relationship with the said client. They also have to keep all documents that are necessary to identify a specific transaction for a period of 10 years, which starts from the date on which the said operation was executed (article 60 *et seq.*).

They must report any transaction, regardless of the amount, when they know or have reasonable grounds to suspect that it is related to money laundering. Moreover, every atypical transaction that was identified in the frame of the risk assessment procedures that have to be implemented by the obliged entities must be thoroughly analysed, notably if the transaction involves a significant amount or if the transaction does not have an apparent economic or legal purpose. This analysis must be recorded in a written report (article 45).

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

See question 3.4.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

See question 3.4.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

The obliged entities must identify the clients with whom they enter into a business relationship or for whom they execute a transaction on an occasional basis, for a total amount of €10,000 or more or in case they execute a transfer of funds in the sense of EU Regulation 2015/847 of €1,000 or more.

To confirm the identity of these clients, the obliged entities must gather evidence that supports the information provided by the clients.

Increased vigilance is imposed when dealing with clients originating from high-risk third countries (countries that have been identified as such by the European Commission on the grounds of article 9 of EU Directive 2015/849), States with no or low taxation or politically exposed persons.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Obliged entities may not enter into a relationship with shell banks under the 18 September 2017 Act (article 40, § 2).

3.9 What is the criteria for reporting suspicious activity?

Obliged entities must report all the funds, operations or facts which they suspect or have reasonable grounds to suspect are linked to money laundering. This obligation to report does not entail an obligation for the obliged entities to identify the predicate offence.

They must also report all suspicious funds, operations or facts in the framework of their activities in another EEE Member State, even when they do not own in such state a subsidiary, a branch or any other kind of establishment through agents or distributors (article 47 *et seq.*).

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Pursuant to article 514 of the Belgian Company Code, any person who acquires or sells securities that confer voting rights in a public limited liability company whose shares are admitted in whole or in part to trading on a regulated market, must declare such acquisition or disposal.

The 18 September 2017 Act has empowered the government to create a Registry of beneficial owners which is accessible to competent authorities, FIUs and obliged entities within the framework of customer due diligence, and any person or organisation that can demonstrate a legitimate interest (article 73 *et seq.*). The practical and procedural aspects of the Registry of beneficial owners have been laid out in the Royal Decree of 30 July 2018 relating to the "UBO" Registry.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

This is indeed the case.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No, it is not.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Anti-money laundering requirements are only imposed on obliged entities, as they have been defined in question 2.1.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Increased vigilance is imposed when dealing with clients originating from high-risk third countries or States with no or low taxation.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

The 5th European AML Directive (2018/843) of 30 May 2018, which entered into force on 9 July 2018, focuses on six main features: (i) designate virtual currency exchange platforms as obliged entities; (ii) set lower maximum transaction limits for certain pre-paid instruments; (iii) enable FIUs to request information on money laundering and terrorist financing from any obliged entity; (iv) enable FIUs and competent authorities to identify holders of bank and payment accounts; (v) harmonise the EU approach towards high-risk third countries; and (vi) improve access to beneficial ownership information. The 5th European AML Directive has not yet been transposed in Belgium and Member States have until the 10 January 2020 to implement the Directive into national law.

Directive 2018/1673 on combatting money laundering by criminal law was adopted on 23 October 2018 and entered into force on 2 December 2018. Its objective is to enable more efficient and swifter cross-border cooperation between competent authorities in the field of criminal law and complements existing criminal national legislations relating to money laundering, which are very limited in scope. Member States have until the 3 December 2020 to implement the Directive into national law.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In 2015, the FATF considered that while Belgium had taken an approach based on risks in its AML activities and initiatives for many years, its understanding of these risks remained fragmented and incomplete. The activities exposed to a high risk of money laundering included the diamond trade, in which Antwerp is a world leading centre, and sectors in which cash circulates, such as the trade in used cars and gold, as well as the money transfer services. The FATF also observed that the geographic position of Belgium makes it a target for the transit of illegal movements of funds. In terms of terrorist financing, the main risks concerned activities relating to 'jihadists' travelling to countries in the Near and Middle East. Continuing radicalisation in segments of the population create undeniable risk. The money transfer sector is particularly vulnerable to these threats.

In its follow-up report of September 2018, the FATF noted that Belgium had made significant progress, which led the FATF to re-rate Belgium positively on 15 recommendations. Belgium is, however, still expected to make progress on 7 FATF recommendations.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Belgium has been evaluated by the IMF in 2014 and by the FATF in 2015.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The 18 September Act 2017 is available in French or Dutch at http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2017091806&table_name=loi.

The 4th AML Directive is available in English at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=FR.

The 5th AML Directive is available in English at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

The website of the Belgian FIU (the CTIF) is also available in English at http://www.ctif-cfi.be/website/index.php?lang=en.

Françoise Lefèvre
Linklaters LLP
rue Brederode, 13
1000 Brussels
Belgium

Tel: +322 501 94 15
Email: francoise.lefevre@linklaters.com
URL: www.linklaters.com

Françoise is a specialist in domestic and cross-border litigation and national and international arbitration.

She has extensive experience in white-collar crime investigations, regulatory investigations, corporate litigation, banking and construction law.

Rinaldo Saporito
Linklaters LLP
rue Brederode, 13
1000 Brussels
Belgium

Tel: +322 501 90 73
Email: rinaldo.saporito@linklaters.com
URL: www.linklaters.com

Rinaldo specialises in domestic and cross-border litigation and national and international arbitration, including white-collar crime, market practices and consumer protection and intellectual property.

Linklaters

Linklaters regularly acts on the most significant regulatory and criminal investigations and related civil disputes in the world – high-value issues that threaten our clients' businesses and reputations. We have a long-standing track record of providing excellent, strategic legal advice on sensitive matters involving anti-bribery and corruption, anti-money laundering, business crimes, fraud, export controls and sanctions, and other related issues.

We are especially well-equipped to address the most challenging cross-border internal investigations and disputes, leveraging our ability to draw upon large multi-disciplinary and multi-jurisdictional teams at short notice. Our collaborative international teams have represented clients before criminal authorities and regulators across multiple jurisdictions and in a wide variety of fields. Our teams have also successfully handled the most sensitive internal investigations.

We have excellent insight into relevant prosecutors and authorities. A number of our lawyers have previously held senior positions at national regulators.

Brazil

Joyce Roysen

Joyce Roysen Advogados

Veridiana Vianna

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In Brazil, the Federal Prosecutor's Office or the State Prosecutor's Office are responsible for prosecuting individuals accused of money laundering at the national level.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

One who wilfully hides or disguises the origin, location, disposition, movement or ownership of goods, rights or money coming from a criminal violation has committed the crime of money laundering under article 1 of Law 9,613/98, with the new wording introduced by Law 12,683/2012. This new wording eliminated the list of predicate offences to the crime of money laundering, instead saying that any crime or criminal violation can be a predicate offence to money laundering, including tax evasion.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

No. As a rule, Brazilian law applies only to crimes committed within Brazil. Under Brazilian law, a crime is considered to have been committed at the location where the act or omission occurred, in whole or in part, as well as where it produced or should have produced its result.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Federal Police and the State Police are responsible for investigating money laundering crimes in police investigations and there are specialised departments for these cases. Additionally, the Federal Prosecutor's Office and the State Prosecutor's Office are responsible for conducting investigations in the Police Inquiries that are within those offices' purview.

1.5 Is there corporate criminal liability or only liability for natural persons?

Brazilian law establishes criminal liability for natural persons only, except in the case of environmental crimes, for which corporations can be held liable. In a criminal proceeding, corporations can be subject to measures affecting their assets, such as seizure, attachment and judicial lien.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Under article 1 of Law 9,613/98, the penalty for money laundering is imprisonment for between three and 10 years and a fine. The penalty can be increased by between one-third and two-thirds if the crime is done repeatedly or through a criminal organisation, under article 1(4) of Law 9,613/98. Legal entities are subject to administrative punishment, in addition to the measures affecting their assets mentioned in question 1.5.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations for money laundering crimes is 16 years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Law 9,613/98 is a federal law. In Brazil, criminal law can only be created at the federal level. States and municipalities cannot legislate on criminal matters.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The judicial branch has the authority to order the confiscation of assets. There are agencies that assist in asset confiscation by providing information, such as the Financial Activity Control Council (*Conselho de Controle de Atividades Financeiras*), or COAF, and the Brazilian Central Bank. The COAF provides

information, has a database and notifies authorities of suspicious financial transactions. The Brazilian Central Bank can freeze money when ordered by the courts. Regarding chattel and real properties subject to confiscation, the Transportation Department and real estate registry offices provide the necessary information and take other measures to record asset seizures ordered by the courts. Article 4 of Law 9,613/98 establishes the legal procedure to seize assets, rights or money of those under investigation for money laundering.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, there are cases of convictions of officers and employees of financial institutions accused of money laundering.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

There is no possibility for settling money laundering crimes without a proper legal proceeding.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The COAF is responsible for disciplining, applying administrative penalties, receiving, examining and identifying occurrences where money laundering is suspected, without limiting the authority of other bodies and agencies. As a rule, the guidelines for fighting money laundering are established by the COAF, which shares monitoring obligations with the agents and regulatory agencies with oversight over specific activities, so as to define the criteria for each type of operation (articles 9, 10 and 14(1) of Law 9,613/98). The COAF must also coordinate the mechanisms for interagency operations to facilitate the fight against hiding or disguising assets, rights and money (article 14(2)), as well as requesting registration and financial information on the persons involved in suspicious activities from the appropriate administrative agencies (article 14(3)).

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

There is no law against private associations establishing corporate governance rules that require anti-money laundering activities beyond compliance and good-conduct rules. In fact, the anti-money laundering law gives private agents certain responsibilities, particularly to improve their records, their operations and communications. In this regard, it is important to note the National Anti-Corruption and Money Laundering Strategy (*Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro*), or ENCCLA, which is an implementing network among federal, state and municipal governments, with participation among the branches of government and various trade associations and is responsible for preparing practical activities to fight and prevent money laundering.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Given that article 9 of Law 9,613/98 lists all the natural persons and legal entities subject to the control mechanisms provided for in it, it is also the duty of self-regulatory organisations to create mechanisms to monitor and fight suspicious activities that might be conducted by their own members, adopting policies, procedures and internal control mechanisms that allow them to meet the obligations established in article 10(III) of Law 9,613/98.

2.4 Are there requirements only at national level?

No. Brazil is a signatory to various international treaties and conventions that establish the parameters regarding this matter, in particular: (i) the Vienna Convention of 1988, promulgated domestically through Decree 154/1991, specifically to fight and prevent money laundering in cases of drug trafficking; (ii) the Palermo Convention of 2000, promulgated domestically through Decree 5,015/2004, which deals with mechanisms to control money laundering as a way of fighting terrorism; and (iii) the Merida Convention of 2003, promulgated domestically through Decree 5,687/2005, which deals with fighting corruption and establishes regulations related to institutions commonly used for this crime.

Additionally, Brazil observes the 40 Recommendations of the FATF-GAFI, a group it has been part of since 2000, guiding the formation of internal control legislation and mechanisms.

At the regional level, Brazil is part of the Financial Action Task Force of Latin America, an intergovernmental regional organisation for mutual evaluations among the members, as well as the development of appropriate mechanisms to improve domestic policies to fight money laundering, beyond the GAFI's 40 Recommendations.

Domestically, and in relation to criminal and administrative rules, the implementation of these measures is carried out at the federal level only, given its legislative authority. However, as mentioned earlier, the establishment of activities and compliance rules at other governmental levels, or even by private entities, is not prohibited.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

In Brazil, compliance policies are established, firstly, in keeping with Central Bank Resolution 2,554/98, when banks operating within Brazil implemented internal control policies over the activities they conduct, their financial information, operating and management systems and the fulfilment of the laws and regulations governing financial institutions.

Thereafter, the duty of compliance was expressly included in the law through article 10 of Law 9,613/98, as amended by Law 12,683/12, which provides that all the persons mentioned in its article 9 must adopt policies, procedures and internal controls that allow them to identify clients and communicate their transactions and operations, if necessary.

The duty of compliance thereby established covers, at the administrative level, the government agencies and authorities with jurisdiction listed in article 9 of Law 9,613/98, as well as the individuals connected to them, through this law's broad implementation.

Even before the effective inclusion of criminal compliance in Brazil's legal and administrative system, policies to prevent and fight money laundering, together with the effective communication of suspicious activity to the authorities with jurisdiction, had already been included through resolutions (for example, COAF Resolution 1 of April 13, 1999) and special laws (for example, Law 9,613/1998). This was later done more specifically and is always done publicly.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

In Brazil, the COAF, which was established by Law 9,613/98, is the Financial Intelligence Unit (FIU) responsible for receiving, storing and organising information, as well as helping fight money laundering through strategic planning.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The statute of limitations is five years from the date on which the fact becomes known to the authority with jurisdiction.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The administrative penalties range from a warning to fines and the cancellation or suspension of authorisation to perform certain activities.

Article 12 of Law 9,613/98 lists the penalties. Monetary fine amounts are: (i) twice the value of the transaction; (ii) twice the actual profit obtained or that presumably would have been obtained by performing the transaction; or (iii) BRL 20 million.

On the other hand, a temporary suspension can be imposed, for up to 10 years, on the right to hold the position of manager of the legal entities referred to in article 9 of the same law, or the authorisation to perform the activity, transaction or function can be cancelled or suspended.

The requirements for the application of penalties can also be seen in the law that governs the COAF. The penalty of a warning will be applied for non-compliance with the instructions referred to in article 10(I) and (II), or in other words, related to the registration of clients and transactions. Fines, in turn, will be levied whenever economic agents, through negligence or wilfully, fail to correct the non-compliance that was the subject of the warning by the deadline given by the authority with jurisdiction, as well as when they fail to comply with their duty of communication. A temporary disqualification will be imposed when they are found to be in serious violation of the fulfilment of obligations established by the COAF, or when there is a specific repetition of infractions previously punished by a fine. Finally, cancellation of the authorisation will be imposed in cases of specific repetition of infractions previously punished by a temporary disqualification.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Both legal entities and individuals, when considered economic agents under the definition in article 9 of Law 9,613/1998, can be subject to the administrative penalties of suspension, temporary disqualification or cancellation of the performance of the economic activity, as provided for in article 7(II) of Law 9,613/98.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No. Individuals are subject to imprisonment for between three and 10 years and a fine. The penalty can be increased from one-third to two-thirds if the crime is committed repeatedly or through a criminal organisation. The penalty can also be decreased if the perpetrator voluntarily cooperates with the authorities, providing information that leads to the investigation of criminal violations, the identification of perpetrators or the location of assets, rights or money that are the objects of the crime.

In addition to imprisonment, a criminal conviction also results in: the loss of assets, rights and money directly or indirectly related to the criminal conduct and the suspension; temporary disqualification; or cancellation of the performance of the economic activity, as mentioned in questions 2.8 and 2.9.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

An administrative decision issued by the COAF in an administrative proceeding can be appealed to the chairperson of the National Financial System Appeals Board (*Conselho de Recursos do Sistema Financeiro Nacional*), or CRSFN, which is the Treasury Ministry unit that serves as the final administrative appeals board.

An administrative proceeding must respect the principle of transparency to which acts performed by the government are subject. One can consult the decisions and administrative appeals filed by financial institutions at the COAF website.

These decisions can also be challenged in court because the Brazilian Constitution provides that the law cannot prohibit the consideration of a threat to or limitation of a right by the courts (article 5(XXXV) of the Brazilian Constitution).

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Article 9 of Law 9,613/98 establishes the activities subject to permanent monitoring by the corresponding legal entity, which is

required to inform the COAF of all suspicious transactions for the purpose of fighting money laundering, with these being referred to as persons subject to the control mechanism.

Legal entities that perform activities related to the following items in Brazil are subject to these obligations: raising, brokering and investing third-party financial resources; and the purchase and sale of foreign currency or gold, instruments or securities. The following are also bound by these obligations: stock exchanges, commodities or futures exchanges and systems for organised, over-the-counter trading; insurers, securities brokers and supplementary pension plans or private equity firms; credit card acquiring banks or administrators, as well as the administrators of consortiums for the acquisition of goods or services; administrators or companies that use cards or any other electronic, magnetic or equivalent means that allow the transfer of funds; leasing and factoring companies; companies that conduct the distribution of cash or any securities, real estate, commodities or services, or that grant discounts for their acquisition, through a drawing or similar method; other entities whose operation depends on authorisation from the regulatory agency for the financial, foreign-exchange, capital and insurance markets; individuals or corporate entities, whether domestic or foreign, who operate as agents, managers, attorneys-in-fact or representatives or in any way represent the interests of a foreign entity that performs any of the activities referred to in this chapter; the individuals or legal entities that perform activities of real estate promotion or the purchase and sale of real properties; individuals or legal entities who sell jewels, stones and precious metals, art objects and antiquities; natural persons or legal entities who sell luxury or high-value items, broker their sale or perform activities that involve a large volume of cash funds; boards of trade and public registries; individuals or legal entities that provide, even on an occasional basis, advising, consulting, accounting, auditing, counselling or assistance services of any nature in the purchase and sale of real properties, commercial or industrial establishments or equity interests of any nature, of the management of funds, securities or other assets, of the opening or closing of banking, savings, investment or securities accounts, the creation, operation or management of companies of any nature, foundations, trust funds or analogous structures, financial, corporate or real estate companies, and the disposition or acquisition of rights over contracts related to professional sporting or artistic activities; individuals or legal entities who work in the promotion, brokering, sale, representation or negotiation of transfer rights of athletes, artists or fairs, expositions or similar events; companies that transport and store valuables; individuals or legal entities who sell high-value assets of rural or animal origin or broker their sale; and the foreign dependencies of the mentioned entities, through their Brazilian head office, in regard to residents in Brazil.

In turn, articles 10 and 11 of Law 9,613/98 state the obligations that must be observed by the institutions subject to oversight: to identify clients and ensure their respective records are updated; to maintain a record of transactions in domestic and foreign currency, instruments and securities, credit instruments, metals or any asset that can be converted into money, that exceed a limit established by the authority with jurisdiction and under the terms of the instructions issued by it; to adopt policies, procedures and internal controls compatible with their size and volume of transactions that are appropriate to meet the legal requirements as regulated by the agencies with jurisdiction; to register with and keep their registration updated with the regulatory agency or, if there is not one, with the COAF, in the manner and under the conditions established by them; and to meet the requirements formulated by the COAF with the frequency and in the manner and under the conditions established by it, with the obligation of maintaining confidentiality regarding the information provided, in accordance with the law.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

In Brazil, there are not yet specific rules regarding monitoring transactions involving cryptocurrencies to prevent them from being used by criminal organisations for money laundering.

However, the Brazilian Ministry of Justice has a specific group to fight corruption and money laundering called the National Strategy for Fighting Corruption and Money Laundering (*Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro*), or ENCCLA, which has been regularly studying the subject of cryptocurrencies as a means of engaging in the crime of money laundering since late 2018. Federal agencies that participate in ENCCLA include the Brazilian Intelligence Agency (*Agência Brasileira de Inteligência*), or ABIN, the Financial Activities Control Council (*Conselho de Controle de Atividades Financeiras*), or COAF, the Brazilian Central Bank and the Federal Police.

Additionally, the Chamber of Deputies (the lower house of Congress) has been debating including a duty to notify COAF in Law 9,613/1998 (Anti-Money Laundering Act) and the monitoring of these transactions by the Central Bank. This would be done through Bill 2,303/2015, which was placed back up for consideration on March 19, 2019, and is currently waiting to go through the hearing and voting process.

In light of the current lack of effective means of analysing and fighting money laundering through cryptocurrencies in Brazil, the best precautions at the moment are: seeking references in foreign laws in force regarding the subject; reinforcing the use of increasing RegTech in processes, which makes available a broad range of auditing and corporate intelligence tools, as well as improving due diligence procedures; and, finally, constant compliance training for those working in the area.

Finally, it should be noted that, at the international level, G20 member governments intend to discuss international regulations against money laundering and the financing of terrorism through cryptocurrencies at a meeting in June 2019, given the importance and relevance of the subject at the global level.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Banking financial institutions have the duty of maintaining internal control systems for the activities they conduct and of instituting compliance policies to prevent money laundering. Central Bank Resolution 2,554/98 establishes the requirement that Brazilian banks have at least one compliance officer, while article 10(III) of Law 9,613/98 provides that "the obligated entities and persons must adopt policies, procedures and internal controls compatible with their size and volume of transactions, that allow them to comply with the provisions of this article and article 11, in the manner regulated by the agencies with jurisdiction".

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Article 10(2) of Law 9,613/98 establishes a minimum period of five years to retain documents from the closing of the account or the conclusion of the transaction, with the guidelines contained in the specific rules issued by the regulatory agencies of the respective individuals and legal entities subject to that law being observed.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Special attention must be paid to transactions that, under the terms of instructions issued by the authorities with jurisdiction, could be evidence of the crimes described in Law 9,613/98, or be related to them. These must be reported to the COAF and no one can be made aware that the report has been made. The authorities with jurisdiction will prepare a list of transactions that, due to their characteristics regarding the parties involved, amounts, manner in which they are conducted, instruments used or lack of economic or legal basis, could be considered illegal.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

According to guidelines from the Brazilian Central Bank, transactions that involve sending funds abroad have minimum requirements to not be considered suspect transactions. For this purpose, the individual or legal entity needs to use an agent authorised to operate in the foreign exchange market and present the document requested of it to carry out the foreign exchange transaction. The agent of the mentioned institutions must inform the interested parties of the necessary procedures, as well as the effective total amount, that takes into account the exchange rate, the Financial Transactions Tax (*Imposto sobre Operações Financeiras*), or IOF, and any fees charged in the transaction. Another option to send and receive funds is the use of an international postal money order, from the Postal Service, in the situations in which this is allowed under foreign-exchange regulations. In general, the maximum amount that can be transferred using this method is established by the Postal Service, respecting the limit provided for in the foreign-exchange regulations of up to the equivalent of USD 50,000 per transaction. For the transfer of funds from abroad to Brazil, it is advisable that, before the money is sent from abroad, the beneficiary contact a foreign-exchange agent, describing the intended transaction, to verify that the beneficiary has the documentation required by the agent, as well as to verify the other conditions for the transaction. It is important to note that funds in foreign currency will not go directly to the account of the beneficiary of the payment order – a foreign-exchange transaction between the beneficiary and the authorised agent will be necessary. The Brazilian Central Bank establishes only that the documentation must be sufficient to support the intended foreign-exchange transaction, with the identification of the clients always being mandatory.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Article 10 of Law 9,613/98 establishes that a person subject to the control mechanisms must identify their clients, keeping an updated record, under the terms of the proper normative instructions, and also requires: that records be kept of every transaction in domestic or foreign currency, instruments or securities, credit instruments, metals or any asset that can be converted into money that exceeds a limit established by the authority with jurisdiction and under the instructions issued by it; that the requirements of the COAF be met; that policies, procedures and internal controls compatible with the scale and volume of transactions be adopted; that an updated registration be created and maintained at the regulatory or oversight agency or, if there is none, at the COAF, with the requirements formulated by the COAF regarding the frequency, manner and conditions being observed, and with the confidentiality of the information provided being preserved under the terms of the law. Moreover, there are specific requirements for certain types of client, such as those who are referred to as politically exposed persons, who as a rule hold public positions, and are listed in COAF Resolution 29 of December 7, 2017.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Shell banks are mentioned in article 52(4) of Decree 5,687 of 2006, which establishes that Brazil will apply appropriate and effective measures, with the assistance of its regulatory and supervisory agencies, to impede the establishment and activity of banks that do not have an actual presence and that are not affiliated with a financial group subject to regulation. This measure seeks to prevent the crime of money laundering. The largest Brazilian financial institutions have a prevention plan and prohibit relationships with shell banks.

3.9 What is the criteria for reporting suspicious activity?

Article 11 of Law 9,613/98 establishes that the person subject to the control mechanism must report to the COAF, within 24 hours, a proposal for or conduct of: any transaction in domestic or foreign currency, instruments or securities, credit instruments, metals or any asset that can be converted into money, that exceeds the limit established by the authority with jurisdiction; and transactions that could be serious evidence of the crime of money laundering.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes. Article 10-A of Law 9,613/98, as well as Law 10,701/2003, establishes that the Brazilian Central Bank will maintain a centralised registry as a general record of account holders and clients of financial institutions, as well as their attorneys-in-fact. The data available for consultation are: identification of the client, its legal representatives and attorneys-in-fact; financial institutions at which the client maintains its assets and/or investments; beginning date; and, if any, ending date of the relationship. Data from this record can be requested by the courts, parliamentary inquiry committees, the COAF and other authorities, when duly authorised and empowered to request information. Information about companies' legal representatives and attorneys-in-fact can be obtained in public databases, such as those of the boards of trade.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes. Brazilian Central Bank Circular 3,461 establishes that financial institutions must adopt measures allowing them to confirm their clients' registration information and identify the final beneficiaries of transactions. Information about account activities and bank transactions cannot be shared between financial institutions because it is confidential. It can be shared with the COAF and police and court authorities, when they are duly authorised and empowered to request information.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Brazilian law does not allow bearer shares for financial institutions or share corporations. Additionally, financial institutions are required to provide all the information about their shareholders and family members to the Brazilian Central Bank.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes, as described in question 3.1, not only financial institutions are subject to the control mechanisms for money laundering.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

As described in question 3.1, not only financial institutions are subject to the control mechanisms for money laundering. However, there is no special requirement to fight money laundering that applies to free trade zones.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Bill 470/17 is currently being considered by the Brazilian Senate, where it awaits analysis by the Constitution, Justice and Citizenship Committee. It would amend Law 9,613/98 and prohibit conducting suspicious transactions with politically exposed persons, or on behalf of such persons, with documentary verification of the origin of the funds handled being mandatory, together with the economic foundation of the transaction and the public economic capacity of the client. This bill would also prohibit cash withdrawals by an individual or legal entity when they exceed, taken as a whole, the amount of BRL 10,000 per day.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

To comply with GAFI/FATF recommendations, Brazil has promulgated Law 12,683/12, which amended Law 9,613/98 and did not provide an exhaustive list of predicate offences to money laundering. It has also promulgated new antiterrorism legislation (Law 13,170/15 and Law 13,260/16). Moreover, the Ministry of Justice and Public Safety, the Solicitor General, the COAF and the Ministry of Foreign Affairs have worked to prepare a bill making United Nations Security Council sanctions directly applicable within Brazil, with the administrative freezing of assets tied to persons and entities listed by it.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

As a full GAFI/FATF member, Brazil has made a commitment to submit to the periodic mutual evaluation process. The IMF also prepares an annual report on the Brazilian economy, which is referred to as "article IV", and this report points out instances of Brazil's progress or failure in relation to fighting money laundering.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Special legislation concerning money laundering can be found on the website of the office of the Brazilian president (http://www.planalto.gov.br), which contains updated official legislation. The same website has the Brazilian Penal Code, which contains the institutes that apply to money laundering legislation. The rules of the Financial Activity Control Council (*Conselho de Controle de Atividades Financeiras*), or COAF, are available on its website (http://www.coaf.fazenda.gov.br/). Other government agencies that help fight money laundering can also be accessed on the internet: (http://idg.receita.fazenda.gov.br/sobre/acoes-e-programas/combatea-ilicitos/lavagem-de-dinheiro; and http://www.bcb.gov.br/pt-br/#!/n/LAVAGEMDINHEIRO).

Joyce Roysen

Joyce Roysen Advogados
Rua Iguatemi, 448 – 17º andar – Itaim Bibi
CEP 01451-010 – São Paulo/SP
Brazil

Tel: +55 11 3736 3900
Email: jroysen@jradvs.com.br
URL: www.jradvs.com.br

Law degree from the University of São Paulo Law School in 1986 – specialisation in criminal law from the University of São Paulo Law School. Yale School of Management – MPL – Management Program for Lawyers. Member of the Brazilian Bar Association since 1987 and Member of the São Paulo Lawyers' Association. Member of the Brazilian Institute of Criminal Science, Member of the International Bar Association (IBA) and Member of the Brazilian chapter of the International Criminal Law Association (AIDP). Council member of the State Human Rights Program of the Secretariat for Public Justice of the State of São Paulo (2002) and recognised as one of the most admired criminal law attorneys in Brazil by the magazine *Análise Advocacia* from 2007 to 2017. Recognised by *Chambers Latin America* 2017/2018 as an outstanding lawyer in the field of business criminal law (Dispute Resolution Brazil – White-Collar Crime).

Veridiana Vianna

Joyce Roysen Advogados
Rua Iguatemi, 448 – 17º andar – Itaim Bibi
CEP 01451-010 – São Paulo/SP
Brazil

Tel: +55 11 3736 3900
Email: vvianna@jradvs.com.br
URL: www.jradvs.com.br

Veridiana Vianna is a partner at Joyce Roysen Advogados (JRADVS) and has a law degree from the Pontifical Catholic University of São Paulo (PUC) in 2008. She also has a graduate degree in criminal law and procedure from the Catholic University of São Paulo (PUC/SP) in 2012. Member of the Brazilian Bar Association, Member of the Brazilian Institute of Criminal Science and Member of the São Paulo Lawyers' Association. Recognised as an admired criminal law attorney by the magazine *Análise Advocacia* in 2017.

JOYCE ROYSEN ADVOGADOS

The firm Joyce Roysen Advogados was founded in 1993.

It is one of the most respected criminal law firms in Brazil, with highly specialised services.

Joyce Roysen Advogados provides legal services in the criminal law area, with a particular focus on business and economic crimes. It defends clients who are under criminal investigation or facing criminal prosecution.

Joyce Roysen Advogados provides both advisory and litigation services to individuals and companies.

Joyce Roysen Advogados' legal advising work focuses on compliance programmes, providing guidance to help clients avoid potential illegal activities.

This work includes advising international clients about Brazilian criminal law.

Canada

Katie Patterson

Vladimir Shatiryan

Blake, Cassels & Graydon LLP

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Section 462.31 of the *Criminal Code* (Canada) creates the criminal offence of money laundering.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

To establish money laundering as a criminal offence, the government must prove, beyond a reasonable doubt, that a person:

1. used, transferred the possession of, sent or delivered to any person or place, transported, transmitted, altered, disposed of or otherwise dealt with, in any manner and by any means, any property or proceeds of any property;
2. with intent to conceal or convert that property or those proceeds;
3. knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of:
   a. the commission in Canada of a designated offence; or
   b. an act or omission anywhere that, if it occurred in Canada, would have constituted a designated offence.

Subject to certain exceptions, a "designated offence" is any indictable offence that may be prosecuted under the Criminal Code or any other federal Act, or any conspiracy, attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an indictable offence. Tax evasion is a designated offence, as it may be prosecuted on indictment.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Money laundering of the proceeds of foreign crimes is punishable under the Criminal Code where the foreign crime, if it had occurred in Canada, would have constituted a designated offence.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Public Prosecution Service of Canada initiates and conducts federal prosecutions of the money laundering criminal offence.

1.5 Is there corporate criminal liability or only liability for natural persons?

Section 462.31 applies to "every one", which includes an organisation.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

If the offence of money laundering proceeds by indictment, the maximum penalty is imprisonment for a term not exceeding 10 years. If the offence proceeds summarily, the maximum penalty is a fine of not more than CAD$5,000 or a term of imprisonment not exceeding six months, or both.

1.7 What is the statute of limitations for money laundering crimes?

If the offence of money laundering proceeds summarily, no proceedings can be instituted more than six months after the time when the subject matter of the proceedings arose, unless the prosecutor and the defendant agree otherwise. If the offence proceeds by indictment, there is no statute of limitations for money laundering crimes.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

The offence of money laundering, as all criminal offences, is prosecuted at the federal level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Section 462.37 of the Criminal Code allows a court to order the forfeiture of certain property. This provision applies if an offender

is convicted of a designated offence, but may also apply if the offender is discharged by the court after pleading guilty to or being found guilty of a designated offence. To impose a forfeiture order, the court must be satisfied, on a balance of probabilities, that the property is the proceeds of crime obtained through commission of the designated offence. If the court is not satisfied that the property was obtained through commission of the designated offence, a forfeiture order may still be made if the court is satisfied, beyond a reasonable doubt, that the property is the proceeds of crime. Property may also be forfeited by order of the court upon sentencing of an offender convicted of certain offences.

Some Canadian provinces have also enacted legislation that enables forfeiture of proceeds of crime through civil enforcement.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

To our knowledge, there are no convictions of regulated financial institutions or their directors or officers for committing the offence of money laundering under the Criminal Code.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The result of negotiations between an accused and the prosecution can be public if those negotiations result in an in-court disposition that includes a plea of guilty. If the prosecution withdraws the charge or agrees to a much less onerous sentence, the result of such negotiations may not be public because they are the result of in-chambers discussions and would not form part of the public record.

Whether certain information is publicly available is very fact-dependent.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Federally, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) imposes anti-money laundering requirements on financial institutions and certain other businesses. The PCMLTFA requires such institutions to maintain a compliance programme, appoint a compliance officer, and conduct an assessment of money-laundering and terrorist-financing risks. Further, the PCMLTFA outlines rules relating to recordkeeping, identity verification, ongoing monitoring and reporting. The PCMLTFA also requires money services businesses to register with FINTRAC, the government entity that administers the PCMLTFA.

In Quebec, the Money-Services Businesses Act (MSB Act) imposes a parallel regulation of money services businesses. The MSB Act requires money services businesses to be licensed with the Autorité des marchés financiers, the regulatory authority that administers the MSB Act.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

The Investment Industry Regulation Organization of Canada (IIROC) is the national self-regulatory organisation that oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. IIROC imposes client identification requirements on its members. Provincial law societies also impose anti-money laundering requirements on their member legal professionals.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Please see our answer to question 2.2 above.

2.4 Are there requirements only at national level?

Yes, the requirements are at the federal level, except in respect of money services businesses, which are also subject to provincial regulation in the province of Quebec.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

FINTRAC is responsible for the examination for compliance and enforcement of the PCMLTFA at the federal level. In February 2019, FINTRAC published an *Assessment Manual*, which outlines FINTRAC's methods for selecting entities for compliance examinations and the process that FINTRAC will follow during examinations.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

FINTRAC is responsible for analysing information reported by financial institutions and businesses subject to the PCMLTFA.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Administrative enforcement actions may not be commenced later than two years after the subject matter of the proceedings became known to FINTRAC. Criminal offences under the PCMLTFA may only be instituted within five years after the time when the subject matter of the proceedings arose if such offences are prosecuted summarily.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum administrative penalty for failure to comply with a requirement of the PCMLTFA is CAD$100,000, if the violation is committed by an individual, and CAD$500,000, if the violation is committed by an entity.

The administrative penalties vary depending on whether the violation is minor, serious, or very serious. A minor violation may result in a penalty up to CAD$1,000, a serious violation may result in a penalty up to CAD$100,000, and a very serious violation may result in a penalty up to CAD$500,000.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

In addition to monetary penalties, FINTRAC may also enter into compliance agreements with persons or entities who have committed a violation.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Violations of anti-money laundering obligations may be subject to criminal sanctions under the PCMLTFA if a person or entity knowingly contravenes certain legislative requirements. However, criminal sanctions are rarely pursued in practice. FINTRAC's preferred enforcement tool is the administrative monetary penalties regime.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

If FINTRAC believes on reasonable grounds that a person or entity has committed a violation, FINTRAC may issue a notice of violation. The notice of violation will state the penalty that FINTRAC proposes to impose, and may also contain an offer to reduce by half the penalty proposed in the notice if the person or entity enters into a compliance agreement with FINTRAC.

The person or entity may choose to pay the penalty, in which case the person or entity is deemed to have committed the violation and the proceedings in respect of it are ended.

Alternatively, the person or entity may make representations to the Director of FINTRAC and the Director will decide whether the person or entity committed the violation. If the violation is serious or very serious, a person or entity will have the right to appeal the Director's decision to the Federal Court of Canada within 30 days after the notice of decision is served.

When proceedings in respect of a violation are ended, FINTRAC may make public the nature of the violation, the name of the person or entity that committed it, and the amount of the penalty imposed.

Entities subject to the PCMLTFA have challenged penalty assessments issued by FINTRAC in the Federal Court of Canada from time to time.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The PCMLTFA applies to the following types of persons and entities:

1. banks and foreign bank branches;
2. credit unions and centrals;
3. life companies;
4. trust and loan companies;
5. securities dealers;
6. money services businesses;
7. intermediaries engaging in certain activities, such as life insurance brokers and agents, British Columbia notaries public and notary corporations, legal counsel and legal firms (subject to limitations), accountants and accounting firms, real estate brokers, sales representatives and developers, and dealers in precious metals and stones; and
8. casinos.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The federal government has introduced amendments to the definition of "money services business" in the PCMLTFA to include persons and entities engaged in the business of dealing in virtual securities. These amendments are not yet in effect.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All persons and entities that are subject to the PCMLTFA must establish and implement a compliance programme. As part of the compliance programme, they must:

1. appoint an anti-money laundering officer;
2. develop and apply written compliance policies and procedures;
3. conduct and document risk assessment;
4. develop and maintain a written, ongoing compliance training programme for employees and agents; and
5. conduct and document an effectiveness review of the policies and procedures, the risk assessment and the training programme. This review must be carried out every two years by an internal or external auditor.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Subject to certain exceptions, persons and entities that are subject to the PCMLTFA must report and keep a record of a transaction where they receive from a client an amount in cash of CAD$10,000 or more in the course of a single transaction, unless the amount is received from a financial entity or a public body. A "single transaction" will include two or more cash transactions of less than CAD$10,000 each if they are made within 24 consecutive hours and total CAD$10,000.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Financial entities, money services businesses and casinos must report the sending out of Canada, or the receipt from outside

Canada, of international electronic funds transfers of CAD$10,000 or more in the course of a single transaction.

Electronic funds transfers that are sent to a person or entity within Canada do not have to be reported, even if the final recipient is outside Canada. Similarly, electronic funds transfers that are received from a person or entity within Canada do not have to be reported, even if the initial sender is outside Canada. For SWIFT messages, only SWIFT MT 103 messages are reportable.

Casinos are also required to report large disbursements of CAD$10,000 or more.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Please see our answer to question 3.5 above.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Financial institutions are required to conduct customer identification when opening an account for a customer and for certain threshold transactions. For individuals, the customer identification must be conducted by using in person or non-face-to-face methods prescribed by legislation. For entities, customer identification is conducted by confirming the entity's legal existence and identifying its authorised signers. Financial institutions are also required to determine an entity's ultimate beneficial owners. The customer identification requirements for other businesses subject to the PCMLTFA are largely similar.

Customers that are assessed to be higher risk must be subject to enhanced customer identification requirements. These enhanced measures are not prescribed.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes. No person or entity may have a correspondent banking relationship with a shell bank, which is defined as a foreign financial institution that does not have a physical presence in any country, unless it is controlled by or is under common control with a depository institution, credit union or foreign financial institution that maintains a physical presence in Canada or in a foreign country.

3.9 What is the criteria for reporting suspicious activity?

Regulated persons or entities must report to FINTRAC every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence. "Reasonable grounds to suspect" is a conclusion that is reached based on an assessment of facts, context and money laundering/terrorist financing indicators. "Reasonable grounds to suspect" is a step higher than "simple suspicion" (i.e., a "gut feeling" or "hunch") and a step below "reasonable grounds to believe" (i.e., there is a probability, supported by verified facts, that an anti-money laundering or terrorist activity financing offence has occurred), according to FINTRAC.

Persons and entities may not disclose (1) that they have made, are making or will make a suspicious transaction report, or (2) the contents of a suspicious transaction report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.

A person or an entity is not liable to criminal or civil proceedings for making a suspicious transaction report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

There is no public registry of beneficial ownership information at the federal or provincial level. The Government of Canada intends to work with the provinces and territories to create a pan-Canadian beneficial ownership registry for all legal persons and entities, including trusts, who have 25% of total share ownership or voting rights. It is not yet clear whether the registry will be publicly available.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Financial entities, money services businesses and casinos that are required to keep a record of electronic funds transfers must include with the transfer the name, address and account number or other reference number, if any, of the client who requested it. This requirement applies to electronic funds transfers, including transfers within Canada that are SWIFT MT 103 messages. Such entities must also take reasonable measures to ensure that any transfer that the person or entity receives includes that information.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The Canada Business Corporations Act prohibits the issuance, in bearer form, of a certificate, warrant or other evidence of a conversion privilege, option or right to acquire a share of a federal corporation.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

As noted in our answer to question 3.1 above, the PCMLTFA applies to certain non-financial institution businesses, such as British Columbia notaries, legal counsel and law firms (subject to limitations), accountants and accounting firms, real estate brokers or sales representatives, dealers in precious metals and stones, real estate developers and casinos.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No, but under Part 1.1 of the PCMLTFA, the Minister of Finance can issue Directives to safeguard the integrity of Canada's financial system. On December 9, 2017, the Minister of Finance issued a Directive on the Democratic People's Republic of Korea, which requires reporting entities to treat all transactions originating from or destined to North Korea as high risk.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

On June 9, 2018, the Department of Finance (Canada) released proposed amendments to the PCMLTFA regulations. The proposed amendments expand the PCMLTFA's application to virtual currencies, businesses providing foreign money services and pre-paid products, among other measures. These amendments are in draft form as of March 2019.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In 2016, FATF released its report discussing its detailed assessment of Canada's anti-money laundering framework. The report concluded that Canada has a strong anti-money laundering and anti-terrorism regime, but requires improvements to be fully effective. The report noted that constitutional constraints limit the ability to fully cover all high-risk areas, such as legal counsel, law firms and Quebec notaries. The report also noted that further supervisory efforts are necessary with respect to the real estate and dealers in precious metals and stones sectors.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

As noted above, FATF released its report discussing its detailed assessment of Canada's anti-money laundering framework in 2016.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The following legislation and administrative guidance is available online:

1. Criminal Code.
2. PCMLTFA (and its associated regulations: Cross-border Currency and Monetary Instruments Reporting Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations).
3. Money-Services Businesses Act (Quebec) (and its associated regulations: Regulation under the Money-Services Businesses Act, Regulation respecting fees and tariffs payable under the Money-Services Businesses Act).
4. FINTRAC Guidance.
5. OSFI Guideline B-8: Deterring and Detecting Money Laundering and Terrorist Financing.
6. *Autorité des marchés financiers* Guidance.

Acknowledgment

The authors would like to thank Jacqueline Shinfield for her invaluable contribution to the writing of this chapter. Jacqueline Shinfield is a Partner in the Financial Services Group at Blake, Cassels & Graydon LLP. Jacqueline advises on all aspects of the payments industry including regulatory compliance issues and consumer protection legislation. Jacqueline has extensive experience advising in respect of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Canadian sanctions legislation. In this regard, she provides advice on the provisions of this legislation and its application and interpretation, prepares and assists clients in audits of their anti-money laundering and sanctions programmes and in preparing industry-specific risk-based risk assessments. Jacqueline also assists clients in making submissions on notices of violation issued by FINTRAC. Jacqueline has been inducted into the Canadian Payments Hall of Fame and is recognised in *The Best Lawyers in Canada*, *Canadian Legal Lexpert Directory*, *Chambers Canada: Canada's Leading Lawyers for Business*, *IFLR1000: The Guide to the World's Leading Financial Law Firms*, and *Acritas Stars* 2019.

Tel: +1 416 863 3290 / Email: jacqueline.shinfield@blakes.com

Katie Patterson

Blake, Cassels & Graydon LLP
199 Bay Street, Suite 4000
Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: +1 416 863 2659
Email: katie.patterson@blakes.com
URL: www.blakes.com

Katie's practice focuses on regulatory compliance for federally and provincially regulated financial institutions. She advises a variety of financial service providers, including Canadian and foreign banks, insurance companies, credit unions, money services businesses and commercial and consumer finance companies.

Vladimir Shatiryan

Blake, Cassels & Graydon LLP
199 Bay Street, Suite 4000
Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: +1 416 863 4154
Email: vladimir.shatiryan@blakes.com
URL: www.blakes.com

Vladimir's practice focuses on a broad range of issues impacting Canadian and foreign financial institutions, including banks, insurance companies, credit unions, financial market infrastructures and payment service providers. He advises on business and ownership structures, establishment of financial institutions and foreign bank branches, cross-border banking rules, permitted investments and activities, bank resolution and recovery laws, regulatory compliance management and governance, payment clearing and settlement laws, and other regulatory issues. Vladimir also has expertise in all aspects of Canada's anti-money laundering legislation and sanctions legislation.

Vladimir has completed a secondment at the Legislation and Approvals Division of Canada's federal banking regulator, the Office of the Superintendent of Financial Institutions.

Blakes

As one of Canada's top business law firms, Blake, Cassels & Graydon LLP (Blakes) provides exceptional legal services to leading businesses in Canada and around the world. Thanks to our clients, Blakes was named the leading law firm brand for the fourth consecutive year and fifth time in the Acritas Canadian Law Firm Brand Index 2019. We also received the most top-tier rankings by practice area of any Canadian law firm in *Chambers Global: The World's Leading Lawyers for Business 2019*. Blakes is recognised as having Canada's pre-eminent financial services practice, including the largest and most active financial services regulatory practice in the country. We provide sophisticated advice to numerous regulated financial institutions, as well as commercial and consumer finance companies, operators of payment systems and other financial-service providers, fintechs, intermediaries, and distributors. We have extensive experience advising all entities subject to Canadian anti-money laundering, anti-terrorist financing and economic sanctions legislation applicable to financial transactions.

China

Chen Yun

Liang Yixuan

King & Wood Mallesons

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering is a criminal offence under Article 191 of the *PRC Criminal Law* (the "Criminal Law"). The *Interpretation of the Supreme People's Court on Several Issues Concerning the Specific Application of Law in the Trial of Money Laundering and Other Criminal Cases* provides further explanations on certain elements of the crime of money laundering.

The People's Procuratorate is the body with legal authority to prosecute money laundering at all levels.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

To establish a crime of money laundering against an offender, the prosecutor shall prove with irrefutable evidence that: (i) there are proceeds generated from predicate offences; and (ii) there are intentions and acts of the offender to dissimulate or conceal the source/nature of such proceeds.

Predicate Offences

Money laundering predicate offences refer to criminal activities in relation to: (i) drugs; (ii) organised crime; (iii) terrorism; (iv) smuggling; (v) corruption & bribery; (vi) disruption of the financial regulatory order; and (vii) financial fraud.

Tax evasion is not a predicate offence of the crime of money laundering. Nevertheless, dissimulating or concealing proceeds generated by the crime of tax evasion will be charged under a separate crime, which is the crime of dissimulating or concealing criminal proceeds.

Knowingly

When determining whether an offender "knowingly" engages in the crime of money laundering, a PRC court will consider both objective and subjective factors, such as:

- the cognitive capacity of the offender;
- how the offender becomes aware of others' criminal activities and/or criminal proceeds;
- the type and amount of the criminal proceeds;
- how the criminal proceeds are transferred or transformed; and
- the offender's statement.

Acts

To be convicted of a crime of money laundering, the offender must have been involved with at least one of the following acts:

- making available accounts;
- assisting others in converting properties into cash, financial instruments or negotiable securities;
- assisting others in transferring funds through bank accounts or other funds settlement channels;
- assisting others in transferring funds offshore;
- assisting others in transferring/transforming criminal proceeds by the way of pawn, rental, sale and purchase, investing, fictitious transactions, false debts, forged security, misrepresenting income, lottery, gambling, and mixing the criminal proceeds with operational revenues of cash intensive businesses such as shopping malls, restaurants or entertainment places;
- assisting others in transferring criminal proceeds offshore/onshore by carrying, transporting or mailing such proceeds; or
- using other ways to transfer/transform criminal proceeds.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The *Criminal Law* gives the PRC authorities extraterritorial jurisdiction over the crime of money laundering:

- committed by the PRC citizens outside of the territory of the PRC;
- committed by foreigners against the PRC or PRC citizens outside of the territory of the PRC; and
- in accordance with international treaties/conventions.

Money laundering of the proceeds of foreign crimes is punishable under the Criminal Law following the above principles.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The public security authorities are responsible for investigating money laundering criminal offences and the People's Procuratorate is responsible for prosecuting these criminal offences.

1.5 Is there corporate criminal liability or only liability for natural persons?

Both institutions (i.e. corporate) and individuals (i.e. natural persons) could be subject to criminal liability of the crime of money laundering.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalty applicable to an individual convicted of money laundering is a 10-year fixed-term imprisonment with a criminal fine of 20% of the amount of laundered money. For an institution, the maximum penalty is a criminal fine of 20% of the amount of laundered money with its directly responsible personnel subject to imprisonment for a fixed term of 10 years.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations for money laundering crimes is 15 years starting from the conclusion of criminal activities.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

The *Criminal Law* is the only criminal code in the PRC and shall be applicable and enforceable across the whole country.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

If a confiscation decision is made by a court, such court is the confiscation authority, and, when necessary, such court may require assistance from the public security authorities in enforcing the confiscation decision. If a confiscation decision is made by an administrative authority, the authority making such decision is the confiscation authority.

For a crime of money laundering, all criminal proceeds and gains obtained in relevant criminal activities are subject to confiscation.

If a People's Procuratorate decides not to prosecute a crime of money laundering but deems the relevant funds shall be subject to non-criminal confiscation, such People's Procuratorate shall form an opinion and hand over the case to another relevant administrative authority (e.g. the PBOC (as defined below)) for further handling.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

We found, in most instances, employees of banks or other regulated financial institutions that have been involved in money laundering activities are convicted under separate crimes (e.g. the crime of corruption, which has a higher maximum sentence). Please note that the PRC court decisions are not all publicly available and we cannot be sure whether or not there are other cases where banks/other regulated financial institutions or their employees are convicted of money laundering.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Money laundering criminal offences cannot be resolved or settled outside the judicial process.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The *PRC Anti-Money Laundering Law* and the *PRC Counter-Terrorism Law* set out systematic anti-money laundering ("**AML**") requirements for all financial institutions established within the PRC and certain non-financial institutions that have AML obligations (together, "**AML Reporting Entity**").

Besides, the People's Bank of China ("**PBOC**"), as the primary regulatory authority of AML issues, has promulgated various regulations and rules that stipulate specific AML requirements for AML Reporting Entities in conducting their businesses (e.g. the *Measures on the Administration of the Customer Identity Verification and the Identification and Transaction Documents Keeping by Financial Institutions*).

The China Banking & Insurance Regulatory Commission ("**CB&IRC**"), and China Securities Regulatory Commission ("**CSRC**"), as the regulators of banking, insurance, and securities sectors, respectively, have also published various rules that impose special AML requirements on financial institutions regulated by these commissions (e.g. the *Implementation Measures of the Anti-Money Laundering Work in Securities and Futures Sectors*).

At a high level, AML requirements can be summarised as follows (note: this is not a complete list):

(i) Customer identity verification obligation – all AML Reporting Entities shall:
- require their customers to provide valid identity certificates;
- regularly review and continuously monitor their customers' identities; and
- re-identify their customers upon the occurrence of certain changes.

(ii) Customer identity and transaction records keeping obligation – all AML Reporting Entities shall:
- retain copies of their customers' identity certificates;
- keep records of their customers' identity information; and
- maintain records of their customers' transactions.

(iii) Reporting obligation – all AML Reporting Entities shall timely report to the local PBOC office and the AML Data Center (as defined below) if:
- their customers refuse to provide valid identity certificates;
- their customers act suspiciously or any transaction is suspicious; and

- the amount of any transaction exceeds the thresholds set out by the authority.

(iv) Other obligations – all AML Reporting Entities shall:

- set up/designate a special department to be put in charge of the AML issues;
- establish a complete AML internal control system; and
- organise AML training.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

There are AML requirements (e.g. a securities company shall ensure that their customers open accounts with such customers' real names) imposed by self-regulatory organisations (e.g. the Securities Association of China).

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Self-regulatory organisations, within their authorities, are responsible for AML compliance and enforcement against their members.

2.4 Are there requirements only at national level?

All requirements mentioned here shall be applicable at all levels.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The PBOC is responsible for compliance and enforcement of all AML requirements. In addition, the CB&IRC and CSRC are responsible for ensuring relevant financial institutions have established complete AML internal control systems and assisting the PBOC in enforcing certain administrative sanctions.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The China Anti-Money Laundering Monitoring & Analysis Center ("AML Data Center") run by the PBOC is the FIU responsible for analysing information reported by all AML Reporting Entities.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The applicable statute of limitations for competent authorities to bring administrative enforcement actions against AML violators is two years starting from the conclusion of the violations.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum administrative fine on an AML Reporting Entity for failure to comply with the regulatory/administrative AML requirements is RMB 5 million and/or such entity could be subject to the revocation of its financial permit. The maximum administrative fine on a directly responsible director, senior manager or employee of an AML Reporting Entity for failure to comply with the regulatory/administrative AML requirements is RMB 500,000 and/or such person could be subject to the revocation of his/her qualification to participate in financial activities and/or be banned from any financial related occupations.

Violations that may trigger the above penalties include but are not limited to:

- failure to establish a complete AML internal control system;
- failure to set up/designate a department to be put in charge of AML work;
- failure to have AML training for employees;
- failure to verify customers' identities;
- failure to retain customers' identity information and transaction records;
- failure to report large-value or suspicious transactions;
- engaging in business with unidentified customers;
- setting up anonymous or fictitious accounts for customers;
- disclosure of information in violation of the duty of confidentiality;
- refusal to cooperate with or obstruct AML investigation; or
- refusal to provide AML investigation materials or provide false materials on purpose.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Besides monetary fines and penalties as outlined in question 2.8, the order for correcting all violations within a time limit can be imposed on AML Reporting Entities and disciplinary sanctions (e.g. a warning) can be imposed on individuals.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

The penalties as outlined in questions 2.8 and 2.9 are only administrative penalties. Violations of AML requirements that trigger the crime of money laundering are subject to criminal sanctions as explained in section 1 above.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

Generally, there are three steps for the PBOC to make an AML sanction decision – discovery, investigation and disposal. If the PBOC discovers/notices any AML violations, it has the authority to investigate relevant AML Reporting Entities or their employees using methods such as questioning relevant persons, compelling entities to provide relevant materials, etc. After the investigation, the PBOC may choose whether or not to impose sanctions and, if so, which sanctions to impose on the relevant entities and/or persons. For violations that trigger the crime of money laundering, the PBOC will hand over the investigation to the public security authority for further handling.

Most resolutions of penalty actions, but not all, by competent authorities are publicly available on the respective competent authorities' websites.

An AML Reporting Entity or an individual may appeal an administrative decision made by a financial regulatory authority to the upper level authority for reviewing the decision or file an administrative action against such authority in a PRC court.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Financial institutions that are subject to AML requirements include:

- all banks and credit cooperatives;
- securities companies, futures companies and fund management companies;
- insurance companies and insurance asset management companies;
- trust & investment companies, asset management companies, finance companies, financial leasing companies, auto finance companies and money brokerage companies; and
- other financial institutions as identified by the PBOC.

Other designated non-financial institutions that are subject to AML requirements include:

- institutions conducting money remittance, exchange, settlement and/or clearing business;
- funds distribution institutions;
- institutions conducting internet finance business;
- real estate development companies, real estate selling agencies, other agencies that provide services in relation to real estate transactions;
- precious metals exchanges that conduct spot trading or provide services for spot trading and traders;
- accounting firms, law firms and notary agencies that handle the following businesses on behalf of their clients – buying and selling real estate, escrowing funds, securities or other assets, escrowing bank accounts and securities accounts, raising funds for establishment and operation of enterprises, and buying and selling business entities;
- service providers that provide professional services for the establishment, operation and management of companies, act or arrange others to act as directors or partners, hold companies' shares, and provide registered addresses, office addresses or mailing addresses to companies; and
- other non-financial institutions as identified by the PBOC.

The PRC AML regime focuses more on what kind of institutions (instead of what kind of activities) shall be subject to AML requirements. There is no consolidated list of activities that are subject to AML requirements. Nevertheless, the authorities, from time to time, issue rules to emphasise AML requirements of certain activities (e.g. establishing cross-border cooperation with a foreign financial institution).

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Issuing and trading of cryptocurrency in the PRC is illegal and forbidden.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

AML Reporting Entities are required to have complete AML internal control systems which shall cover all AML requirements as outlined in question 2.1.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

In respect of recordkeeping, an AML Reporting Entity is required to keep records of all transactions for at least five years, regardless of the value of the transaction.

In respect of large cash transactions reporting, an AML Reporting Entity shall report if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 50,000 (included), or USD 10,000 (included) or the equivalent.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

In respect of other large-value transactions, AML Reporting Entities shall also report:

- for fund transfers of institutional customers, if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 2 million (included), or USD 200,000 (included) or the equivalent;
- for onshore funds transfers of individual customers, if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 500,000 (included), or USD 100,000 (included) or the equivalent; and
- for cross-border fund transfers of individual customers, if the value of a single transaction or the accumulated value of various transactions within a day exceeds RMB 200,000 (included), or USD 10,000 (included) or the equivalent.

AML Reporting Entities shall also report suspicious transactions (please refer to question 3.9).

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Criteria for reporting cross-border large-value transactions are outlined in questions 3.4 and 3.5. Criteria for reporting cross-border suspicious transactions are outlined in questions 3.9.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

General customer identification and due diligence requirements for AML Reporting Entities include but are not limited to:

- for institutional customers, verifying the name, address, scope of activities, valid licences proving the lawful establishment of the institution, shareholding structure, constitutional documents (including registration certificate, partnership agreement, articles of association, etc.), information of institutional shareholder or directors, and name, valid ID of the controlling shareholder/person, beneficiary owner, legal representative, responsible manager and authorised agent; and
- for individual customers, verifying the name, gender, nationality, occupation, residence/place of working, contact, and valid ID.

Enhanced customer identification and due diligence requirements for AML Reporting Entities include but are not limited to:

- for institutional customers whose shareholder is another institution, tracking down the individual who is the controlling person or beneficiary owner of such institutional customers, and verifying and registering information of each beneficiary owner;
- for institutional customers with high risk, verifying the beneficiary owner of such customers with even more stringent standards; and
- for individual customers who have special standings (e.g. senior managers of international organisations and officers of foreign countries), verifying the special standings of these customers, obtaining senior managers' approval before taking in such individuals as customers, understanding assets of such customers and sources of such assets, and enhancing the frequency and intensity of transaction monitoring.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

All financial institutions are strictly prohibited from opening any account for or developing any cooperation with foreign banks which have no actual business activities in the countries where they are licensed and are under no effective supervision.

3.9 What is the criteria for reporting suspicious activity?

All AML Reporting Entities shall report suspicious transactions. Suspicious transactions refer to all transactions, regardless of the value involved, that an AML Reporting Entity has reasonable cause to believe that such transactions or any person engaged in such transactions are related to criminal activities. AML Reporting Entities shall formulate their internal transactions monitoring standards in accordance with the requirements of the law, use such standards to identify every suspicious transaction and report every identified suspicious transaction to the local PBOC office and the AML Data Center.

Specifically, all AML Reporting Entities must report a transaction if the transaction:

- is related to money laundering, terrorism financing or other criminal activities;
- will jeopardise national security or social stability;
- is linked to other serious situations or emergencies; or
- is related to anyone on the list of terrorism organisations and terrorists as published by the PBOC, the United Nations Security Council, or other organisations that the PBOC requires all entities to pay attention to.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The State Administration for Market Regulation maintains current and adequate institutional information of all corporates established within the PRC. Other authorities also publish information of special licences approved by such authorities.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Accurate information about originators and beneficiaries must be included in payment orders for all fund transfers. Such information shall also be included in payment instructions to other financial institutions.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The *PRC Company Law* permits joint-stock companies to issue bearer shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

There are specific AML requirements applied to non-financial institution businesses.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

More attention is required to be paid to high-risk business sectors (e.g. international trade).

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

The PRC has a plan to build a complete AML/CTF legal regime by the year of 2020. There are several AML measures under consideration/trial implementation.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In the FATF's Mutual Evaluations Report of China (2012), the FATF concludes that the PRC has taken sufficient action to bring its compliance to a level essentially equivalent to most of FATF's recommendations and has made progress in addressing the deficiencies. To date, FATF has not published any new report on China.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

FATF has a scheduled onsite visit to the PRC around 2018/2019, but, to date, the new evaluation report has not been published.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Most AML rules are available on http://www.pbc.gov.cn/fanxiqianju/135153/index.html. Websites of the State Council, PBOC, CB&IRC and CSRC also publish relevant AML laws, regulations and rules issued, respectively, by each of these authorities. These materials are not published in English but English versions can be found in the FATF's Mutual Evaluations Report of China and other resources.

Chen Yun

King & Wood Mallesons
17th Floor, One ICC
Shanghai ICC, 999 Huai Hai Road
Xuhui District
Shanghai 200031
P.R. China

Tel: +86 21 2412 6052
Email: chenyun@cn.kwm.com
URL: www.kwm.com/zh/cn

Mr. Chen Yun is a partner at King & Wood Mallesons specialising in banking, finance, foreign exchange and AML laws.

His practice includes general banking matters, financial compliance matters, syndicated lending, import and export credit facilities, international financial leasing, and receivables finance, among other areas.

He has extensive experience in assisting and advising foreign banks on their daily operations and business expansion in China. Mr. Chen regularly renders legal advice on: the PRC regulatory requirements for AML compliance; marketing foreign banks' new products; structuring, negotiating and documenting transactions involving the banks' products; standardising bank daily operational documentation for matters such as opening accounts, credit extensions, securities, trade finance and derivatives; and assisting foreign banks in establishing, reorganising, and expending their business presence in China.

Mr. Chen Yun has been ranked as one of the leading individuals in banking and finance areas by *Chambers & Partners* for many years.

Liang Yixuan

King & Wood Mallesons
17th Floor, One ICC
Shanghai ICC, 999 Huai Hai Road
Xuhui District
Shanghai 200031
P.R. China

Tel: +86 21 2412 6447
Email: liangyixuan@cn.kwm.com
URL: www.kwm.com/zh/cn

Ms. Liang Yixuan is an associate of Mr. Chen Yun at King & Wood Mallesons specialising in banking, foreign exchange and AML laws.

She has experience in assisting and advising foreign banks on their daily operations and compliance matters in China. Ms. Liang regularly renders legal advice on: the PRC regulatory requirements for AML compliance; marketing foreign banks' new products; documenting transactions involving the banks' products; and standardising bank daily operational documentation for matters such as opening accounts, credit extensions, securities, trade finance and derivatives.

KING&WOOD MALLESONS
金杜律师事务所

Recognised as one of the world's most innovative law firms, King & Wood Mallesons offers a different perspective to commercial thinking and the client experience. With access to a global platform, a team of over 2,000 lawyers in 27 locations around the world works with clients to help them understand local challenges, navigate through regional complexity, and to find commercial solutions that deliver a competitive advantage for our clients.

As a leading international law firm headquartered in Asia, we help clients to open doors and unlock opportunities as they look to Asian markets to unleash their full potential. Combining an unrivalled depth of expertise and breadth of relationships in our core markets, we are connecting Asia to the world, and the world to Asia.

France

BONIFASSI Avocats

Stéphane Bonifassi

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Public Prosecutor with each local Court is in charge of prosecuting money laundering. A Special Prosecutor for Financial Crimes (*procureur de la République financier*) also has authority to prosecute money laundering at national level in cases where sums being laundered have been obtained through a certain set of offences, including corruption, embezzlement of public funds or tax evasion.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

A distinction should be made between the general offence of money laundering, provided for under article 324-1 of the Criminal Code, and the various special money laundering offences under the Criminal Code, the Customs Code and the Monetary and Financial Code.

In the event of proceedings under article 324-1 of the Criminal Code, which is divided into two sub-paragraphs, the government must first establish, as *actus reus*, that the accused has (1) facilitated, by any means, the fraudulent justification of the origin of the property or income of the author of a crime or an offence, which generated a direct or indirect profit, or (2) that the defendant assisted in the placement, concealment or conversion of the direct or indirect proceeds of an offence.

Under article 324-1 (1), it should be noted that means of facilitation need not be fraudulent. Further, the prosecution does not have to prove that the property or income whose origin has been falsified are the actual proceeds of a crime or offence. The prosecution only has to prove, on one hand, that there was a fraudulent justification of the origin of property or income, and, on the other hand, that the owner of said property or income is the author of a crime or offence, which generated a direct or indirect profit.

Under article 324-1 (2), however, the prosecution must establish that the accused assisted in placing, concealing or conversing sums, which were the direct or indirect proceeds of a crime or offence.

For both, the government must establish the *mens rea* of the accused, that is, it must be proven that the accused knew of the illegal origin of the property, but it is not necessary to establish knowledge of the specific crime or offence.

In any case, it must be proven that a predicate offence has been committed which is likely either to have produced a "direct or indirect profit" (article 324-1 sub-paragraph 1) or generated "direct or indirect proceeds" (article 324-1 sub-paragraph 2).

With the exception of petty offences, any offence may constitute a predicate to money laundering, such as tax evasion. On this point precisely, it was, until Act no. 2018-898 of October 23, 2018, required from the French tax administration to apply to the Commission on tax offences before reporting tax offences for prosecution. The French tax administration is now under an obligation to automatically report under certain circumstances for prosecution tax offences over €100,000, or €50,000 where the alleged offender was under specific disclosure and transparency obligations. In any case, there was, and there still is no such requirement for prosecution of money laundering charges of tax evasion proceeds.

The predicate offence need not have been prosecuted, and it does not matter that prosecuting the predicate offence in France is impossible, including, for example, if the statute of limitations has run.

As to the standard of proof regarding the existence itself of a predicate offence, courts first required that the predicate offence be established in all its components by the prosecution.

However, over the last 10 years, courts of appeals and the *Cour de cassation* have upheld convictions of money laundering in cases where the predicate offence had only been identified by the prosecution, but not established in all its constituent elements.

The burden of proof on the prosecution has further been lowered since Act n°2013-1117 of December 6, 2013, which created article 324-1-1 of the Criminal Code. Under this provision, property or income is considered, until proven otherwise, to be the direct or indirect proceeds of an offence if the material, legal or financial conditions of the investment, concealment or conversion operation can have no other justification than to conceal the origin or beneficial owner of such property or income. It is the defendant's responsibility to provide evidence that funds or property were lawfully obtained.

Although article 324-1-1 expressly reverts to article 324-1 for application, without distinction between subparagraphs 1 and 2, its scope has been limited to prosecutions for money laundering under article 324-1, subparagraph 2, as it solely refers to operations of "*placement, concealment or conversion of the direct or indirect proceeds of an offence*".

Even so, it is now possible to prosecute and convict on money laundering charges without any reference to a specific predicate offence.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

French courts have jurisdiction over all offences committed in France (mainland and overseas territories) as well as over offences committed by a French national abroad, although there is, with the exception of the most serious crimes, a condition that the conduct must be punishable under the legislation of the country in which it was committed.

Courts also have jurisdiction over offences committed abroad against a French national.

There is, as such, extraterritorial jurisdiction over the crime of money laundering.

However, according to a recent court decision, there would also be extraterritorial jurisdiction over money laundering when this offence is not separable from its predicate offence committed in France.

In a recent case involving a bank registered under the laws of San Marino, which had been indicted for fraud committed in France and for money laundering the proceeds of that fraud committed abroad, the *Cour de cassation* (court of last resort over judicial matters) held that the bank could be indicted in France on charges of money laundering committed abroad, as it was not separable from the predicate offence of fraud committed in France.

This decision might be regarded as contrary to a general trend in court rulings that consider money laundering to be distinct from its predicate offence. Especially so, as it is in reference to this principle that French courts have upheld their jurisdiction over money laundering of proceeds of foreign crimes.

Courts have indeed repeatedly ruled that statutes defining money laundering do not require that the predicate offence be committed in France, nor do they require that French courts have jurisdiction over it. As long as one of the constituent elements of money laundering was committed in France, French courts have jurisdiction (article 113-2 of the Criminal Code).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Investigations are led by the police, usually a special division tasked with combatting fraud, money-laundering and other financial crimes, either under the supervision of the local public prosecutor or the special prosecutor for financial crimes.

An investigative judge may also conduct investigations on money laundering charges where the case is especially complex, or if the prosecutor has refused to investigate or has not initiated criminal proceedings three months after an official complaint of a victim, and after the victim has confirmed their will to proceed.

It should be noted that a draft amendment extending this three-month period to six months is currently under consideration.

1.5 Is there corporate criminal liability or only liability for natural persons?

Both legal entities and natural persons can be prosecuted and convicted for money laundering. As far as legal persons are concerned, their liability can only be retained on the basis of acts committed by their officers, directors or representatives.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

For natural persons, the maximum penalties for a money laundering conviction are five years of imprisonment and a €375,000 fine. However, under article 324-3 of the Criminal Code, the amount of the fine may be raised up to half the value of the property or funds for which the money laundering operations were carried out.

As to legal entities, the maximum penalty applicable is a €1,875,000 fine, which may equally be raised up to 250% of the value of the property or funds object of the money laundering operations.

It should be noted that penalties for legal entities may also include dissolution or prohibition to exercise, directly or indirectly, one or more social or professional activities, either permanently or for a maximum period of five years.

Money laundering is aggravated under certain circumstances. Penalties for natural persons are increased to 10 years of imprisonment and a €750,000 fine. Again, this amount may be raised up to half the value of the property or funds for which the money laundering operations were carried out.

However, according to article 324-4 of the Criminal Code, in cases where the predicate offence carries a term of imprisonment exceeding the term of imprisonment for money laundering, and the defendant had knowledge of the predicate offence, the applicable penalty to the money laundering charges is the penalty attached to the predicate offence. This applies to the aggravating circumstances of the predicate offence as well. In some of those cases, therefore, the maximum penalty for money laundering is life imprisonment.

For legal entities, the maximum penalty for aggravated money laundering is a €3,750,000 fine.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations for prosecuting money laundering was previously three years. A new legislation, which came into force on March 1, 2017, provides for a statute of limitations of six years from the day on which the offence was committed. Where the existence of an offence is concealed, the statute of limitations of six years runs from the day on which the offence became apparent and could be established under conditions allowing for prosecution. In this case, no prosecution is possible after 12 years.

All money laundering offences for which the statute of limitations had run before that date are not impacted by the reform.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

To the extent that France is not a federal state, the issue of parallel state or provincial criminal offences is void.

However, enforcement is not centralised at national level but handled by prosecutors with local courts with the exception of prosecutions led by the Special Prosecutor for Financial Crimes. Still, local prosecutors can investigate in all French territories.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Pursuant to articles 131-6, 131-21, and 131-39 of the Criminal

Code, all or part of the assets of a natural or legal person can be forfeited if there has been a criminal conviction for money laundering.

All assets can be subject to forfeiture, either movable assets or real estate, including jointly owned property.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

There is some case law of bank or financial institution employees being convicted for money laundering. With regards to banks or financial institutions themselves, a much more recent case from the Paris criminal court is worth noting: on February 20, 2019, the Swiss bank UBS AG has been found guilty of aggravated money laundering by the criminal court of Paris, and convicted to a fine of €3.7 billion, in addition to €800 million in damages to the French State. UBS France was also found guilty of aiding and abetting money laundering and convicted to a €15 million fine. UBS has indicated it intended to appeal against this verdict.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Charges of money laundering against a natural or legal person may be settled outside of court, if certain conditions are met.

The prosecution may offer a plea agreement (*comparution préalable sur reconnaissance de culpabilité*) where the defendant, either a natural or legal person, is charged with money laundering. The defendant must plead guilty in exchange for a reduced sentence. Terms of imprisonment cannot in any case exceed three years (it could not exceed one year of imprisonment, until much recently and the enactment of Act n°2019-222 of March 23, 2019), nor can the amount of the fine exceed the maximum amount incurred. In January 2016, the Swiss bank REYL, charged in France with money laundering of tax fraud proceeds agreed to plead guilty and was sentenced to a fine of €2,800,000.

At the discretion of the prosecution, a lighter guilty plea (*composition pénale*) is available to natural persons, but only in cases where charges are brought for misdemeanours carrying up to five years in prison. Sentences available to the prosecution do not include prison terms. Charges of money laundering, which can carry a maximum of five years in prison, may technically be settled through a *composition pénale*, although it is unlikely considering how complex and serious these charges often are.

Both of these agreements must be approved by a judge in open court.

Act n°2016-1691 of December 9, 2016 incorporated into French criminal procedure the *Convention Judiciaire d'Intérêt Public* (CJIP), a new kind of settlement not far from the American deferred prosecution agreement, for legal entities charged with corruption, influence peddling, money laundering and other specific offences.

This deal is offered by the prosecution and at its discretion, as long as criminal proceedings are not under way, or in cases of indictment and under certain circumstances, by an investigative judge.

It is not a guilty plea *per se*, as no admission of guilt is required.

The legal person can undertake one or more of the following obligations:

- payment of a fine to the Treasury not exceeding 30% of its turnover;
- setting up a compliance programme under the supervision of the French anti-corruption agency (ACA), for a maximum period of three years; and
- compensation for identified victims.

It must be approved in an open court.

In October 2017, facing charges of money laundering of tax evasion proceeds, HSBC Private Bank concluded a CJIP with the Special Prosecutor for Financial Crimes, agreeing to a fine and damages for a total of €300,000,000. Interestingly, the UBS group had also been offered a CJIP from the Special Prosecutor for Financial Crimes on charges of money laundering of tax evasion proceeds. The deal offered by the Special Prosecutor, which UBS ultimately refused, was a little over €1 billion. UBS had challenged the amount of the financial penalty offered by the prosecutor as being disproportionate to the offences allegedly committed. As pointed out above, UBS AG ended up being convicted over three times the amount (as mentioned above, an appeal is pending).

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Anti-money laundering requirements on financial institutions and other business are imposed by law at a national level. These obligations are set out in the French Monetary and Financial Code.

In addition, the *Autorité de contrôle prudentiel et de resolution* (ACPR) has set out additional AML requirements on financial institutions and other businesses, such as Instruction 2017-I-11, applicable to banking and insurance institutions.

Requirements include:

- customer due diligence, with a duty to clearly identify the client or beneficial owner of funds or transactions;
- the obligation to report specific transactions or suspicious operations and activities;
- the obligation to keep information records for a period of time; and
- the obligation to set up internal compliance programmes.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Organisations and professional associations may provide guidelines or impose ethical obligations regarding anti-money laundering.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

For persons subject to AML requirements, article L. 561-36 of the Monetary and Financial Code provides a list of professional associations and self-regulatory organisations responsible for controlling compliance by their members. One example of these is the Bar Council for attorneys.

2.4 Are there requirements only at national level?

To the extent that France is not a federal state, there are no parallel state or provincial anti-money laundering requirements other than those imposed at a national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Authorities in France charged with ensuring compliance by financial institutions with AML requirements are:

- the *Autorité de contrôle prudentiel et de resolution* (ACPR) under the supervision of the *Banque de France* (French Central Bank), for credit and payment institutions, investment firms, insurance and mutual insurance companies, insurance intermediaries, and money exchangers; and
- the *Autorité des marchés financiers* (AMF), for portfolio management companies, crowdfunding companies and other investment firms.

These authorities may carry off-site or on-site inspections, take administrative measures or sanctions against the financial institutions themselves as well as their directors, employees, officers, and all those acting on behalf of the entity. Both these authorities provide public information on their criteria and conditions for examination and imposing sanctions.

The *Commission nationale des sanctions* (national committee on sanctions) established under the authority of the Ministry of the Economy, is an independent institution that can take sanctions against certain professionals, including real estate agents and gambling or betting operators, for failing to comply with AML requirements. Pursuant to Decree n°2018-284 of April 18, 2018, sanctions rendered by the *Commission nationale des sanctions* are now to be publicly available, with names of companies and persons involved no longer redacted.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Intelligence Processing and Action against Illicit Financial Networks Unit (TRACFIN) is responsible in France for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitations applicable to enforcement actions before the sanctions committee of the ACPR. It has been frequently challenged by defendants to proceedings before the authority. The *Conseil constitutionnel* (French Supreme Court on questions of constitutional law) has held that there is no constitutional principle imposing a statute of limitation to disciplinary proceedings.

There is, however, a three-year statute of limitation regarding enforcement actions before the sanctions committee of the AMF pursuant to article L. 621-15 of the Monetary and Financial Code.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum sentence is a fine of €5 million before the *Commission nationale des sanctions*.

Before the ACPR, a financial penalty of up to €100 million may also be imposed, although a ceiling of 10% of the net annual turnover is provided for most institutions. A financial penalty of €5 million may also be imposed against natural persons.

The maximum is of €100 million or 10 times the amount of any profits made before the sanctions committee of the AMF. For natural persons, the maximum penalty incurred is a fine of €300,000 or of five times the amount of profits made.

Non-compliance with one or several of the AML requirements provided in the Monetary and Financial Code is cause for sanction.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Other sanctions include warnings, reprimands, bans on carrying out certain operations for a maximum period of 10 years, temporary suspension of directors for a maximum period of 10 years, or withdrawal of a licence.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

There may also be criminal sanctions. The Monetary and Financial Code applies criminal sanctions for:

- violating non-disclosure requirements under articles L. 561-19 and L. 561-26 (III), as well as non-disclosure requirements with regards to information collected by TRACFIN; and
- obstructing and impeding the authority, in any ways including the failure to respond to formal information requests by the authority. This violation carries a maximum penalty of one year in prison.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

Decisions imposing sanctions rendered by the *Commission nationale des sanctions*, the AMF, and the ACPR are collected and made available to the public on their respective websites.

The *Conseil d'Etat* (Supreme Court on administrative matters) hears appeals of decisions rendered by the ACPR and the *Commission nationale des sanctions*.

The *Conseil d'Etat* also hears appeals of decisions of the AMF against any person subject to the authority's supervision according to article L. 621-9 II of the Monetary and Financial Code. The Paris Court of Appeal has jurisdiction over all other appeals.

Rulings by the *Conseil d'Etat*, the Paris Court of Appeal and the *Cour de cassation* regarding sanctions imposed on financial institutions by the AMF are both available on the authority's website.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Institutions and other businesses subject to anti-money laundering

requirements are listed under article L. 561-2 of the Monetary and Financial Code.

Targeted financial institutions are those in the banking sector, including electronic money institutions, insurance companies and intermediaries, mutual societies and unions, the *Banque de France*, investment firms and money changers, among others.

Other professional activities include real estate agents, accountants, auditors, auction sellers, sport agents and lawyers.

Aside from these specific requirements, under article L. 561-46 §1 of the Monetary and Financial Code, all companies and economic interest groups registered in France, as well as all foreign commercial companies with a branch in France and all other legal entities required by law to register in France, have an obligation to (1) obtain and maintain accurate and up-to-date information on their beneficial owners, and (2) to file at the court registry a document identifying the beneficial owner and the type of control over the legal entity that is exercised.

These new obligations, stemming from Ordinance n°2016-1635 of December 1, 2016 implementing the EU fourth Anti-Money Laundering Directive n°2015/849 of May 20, 2015, are not applicable to companies listed on a regulated market in France, the EU, or in a country with similar legislation.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Since December 2016, France has subjected cryptocurrency exchange platforms to anti-money laundering obligations pursuant to article L. 561-2 (7°*bis*) of the French Monetary and Financial Code, but the extent of anti-money laundering obligations on the entire industry has otherwise arguably been limited. However, while the EU Directive 2015/849 of May 20, 2015 did not provide for specific regulations of this industry, the following EU Directive 2018/843 of May 30, 2018 is now imposing on Member States to provide anti-money laundering obligations for exchange platforms and custodian wallet providers by January 20, 2020.

It is worth noting, in addition, that TRACFIN (the French Financial Intelligence Unit) has indicated in its latest report on the years 2017–2018 that it had created a new unit on financial cyber-criminality of dedicated investigators focused on the cryptocurrency industry. The French Parliament is currently working on new and reinforced regulations for this sector (Loi PACTE).

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

As provided by article L. 561-32 of the Monetary and Financial Code, institutions and persons listed in article L. 561-2 of the same Code are compelled to set up internal risk assessment and management programmes, under the conditions defined by law or, in the absence thereof, by regulations of the competent supervisory authority.

Namely, for financial institutions other than insurance intermediaries or those falling under the purview of the *Autorité des Marchés Financiers*, compliance implies that they:

- name a member of management as a reporting officer;
- determine money laundering and terrorist financing risks presented by their activities;
- determine, if necessary, a profile of the business relationship with the client in order to detect anomalies;
- define applicable procedures in risk management, customer due diligence measures, document retention, detection of unusual or suspicious transactions and compliance with the TRACFIN reporting obligation;
- implement periodic and ongoing internal controls; and
- take into account money laundering risks in recruiting staff, according to the level of responsibilities exercised, and organise staff training.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Since October 1, 2013, payment institutions, credit institutions, and electronic currency institutions must systematically report to TRACFIN information regarding large cash or electronic currency transfer transactions. The threshold is hereof €1,000 per transaction, or €2,000 per customer over one calendar month. The report must be filed within 30 days following the month when the transaction took place.

The same institutions are under a similar obligation, as of January 1, 2016, regarding cash payments or withdrawals to or from a deposit or payment account, which exceed €10,000 over one calendar month.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Financial institutions must automatically report information on transactions that present a high risk of money laundering or of financing terrorism, due to (1) the country to or from which funds are being transferred, (2) the nature of the transaction, or (3) the nature of the legal structure or scheme surrounding the transaction. Trusts are specifically targeted by this measure.

This reporting obligation does not preclude these financial institutions from reporting suspicious operations.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There is an obligation for natural persons to report to customs any cross-border transfer of money, securities, or stock of an amount exceeding €10,000.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Persons and legal entities subject to anti-money laundering requirements must exercise due diligence before entering into a business relationship as long as it is ongoing.

Namely, under article L. 561-5 of the Monetary and Financial Code, they must:

1) Before entering into a business relationship or assisting in the preparation or execution of a transaction, identify their client and, where applicable, the beneficial owner of the client or the transaction. Identification is based on any reliable written document, such as identification documents for a natural person, and certificates of registration or statutes of incorporation for legal entities.

2) Verify the identity of their occasional customers and, where appropriate, of their beneficial owners, when they suspect that a transaction could participate in money laundering or terrorist financing, or when the transactions are:
   - of an amount of over €15,000 for any person other than money changers and legal representatives of casinos and other related institutions;
   - of an amount of over €8,000 for *bureaux de change*; and/or
   - of any amount in cases of money transfer or manual foreign exchange transactions, if the client or his legal representative is not physically present, or when offering safe custody facilities.

During the business relationship, they must keep and update the relevant information regarding their clients and transactions. Collected information must be kept for a period of five years following the date of closure of accounts or of the termination of the business relationship.

There is a simplified duty of due diligence when (1) the client or beneficial owner, or (2) the purpose of the transaction of nature of the contract present a low risk of money laundering.

There is conversely an enhanced due diligence requirement when there is a higher risk of money laundering with regards to the client or beneficial owner of the transaction, or its purpose or nature.

Finally, financial institutions may rely on a third party, a list of which is provided by law, in identifying clients and beneficial owners, and for collecting information pertaining to the nature and purpose of transactions. Financial institutions relying on a third party must have full access to the collected information and remain liable in cases of violation of due diligence requirements.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Banking institutions listed under article L. 561-2 (1) and (5), as well as the *Banque de France* are prohibited from offering correspondent banking services with a credit institution, or any other entity engaging in similar activities, in a country where the latter has no effective physical presence, with no management, if not affiliated to a regulated institution or group.

3.9 What is the criteria for reporting suspicious activity?

As provided under article L. 561-15, I of the Monetary and Financial Code, persons and institutions listed under article L. 561-2 of the same Code must report suspicious transactions or funds, which they know, suspect, or have good reason to suspect are the result of an offence carrying a prison sentence of more than one year or linked to financing terrorism.

Courts have held that an activity is suspicious when the lawful origin of funds could not be established after adequate examination by the person or institution, and should as such be reported.

Specifically, courts examine the nature and amount of transactions between legal entities or with natural persons, as well as whether these transactions are consistent with (1) other transactions usually made to or from the person's bank account, and (2) the corporate object of the legal entity and the amount of its capital.

According to a recent decision by the *Cour de cassation*, for instance, currency transactions of several hundred thousand euros to and from a legal entity's bank account, and to accounts belonging to a Belgian company and several natural persons, even where it is consistent with both the corporate object of the legal entity and its capital amount, and where such transactions are not unusual on said account, may raise suspicion of money laundering (*Cour de cassation*, *chambre commerciale*, case n°14-24.598, May 3, 2016).

Under article L. 561-15, II, there are more demanding criteria applying to reports of suspicion of tax evasion, an offence which also carries a prison sentence of more than one year. In such cases, suspicious activity must only be reported if at least one of the criteria defined by law has been met; for example, if there were a deposit by a natural person of funds unrelated to his or her professional activity or known assets.

The reporting duty of article L. 561-15 also covers attempted transactions, including in cases of tax evasion where at least one of the criteria listed in article 1741 of the Tax Code has been met.

Any information that either confirms or dispels the suspicious nature of the activity must be reported to TRACFIN without delay.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

There is, as of April 1, 2018, a new obligation for most companies or legal entities in France to provide accurate and up-to-date information on their beneficial ownership. This information is collected in a registry, which is made available to authorities and to persons and legal entities subject to AML requirements. Decree no. 2018-284 has extended entities subject to the obligation to declare relevant beneficial ownership information, expressly requiring a declaration obligation in cases of trusts (the new article R561-5 of the Monetary and Financial Code uses the terms "*fiducie* or comparable legal arrangement under foreign law"). There are also no longer any exemptions from having to identify the ultimate beneficial owner of a business relationship, but for publicly-traded companies in the European Union, European Economic Area, or in a third country imposing obligations recognised as equivalent by the European Commission within the meaning of Directive 2004/109/EC.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Regulation (EU) 2015/847, applicable in France, set out specific requirements on any provider or an intermediary payment service provider established in the European Union with regards to information included in payment orders or funds transfers.

Some exceptions aside, payment service providers must ensure that orders for transfers of funds are accompanied with the following information:

- name and account number of both payer and payee; and
- payer's address, official personal document number, customer identification number or date and place of birth.

It is interesting to note that transfers of funds between France and Monaco, the latter of which is arguably a tax haven, are treated as transfers of funds within the French Republic. As such, required information is limited to the account numbers of payer and payee.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Stricto sensu, ownership of legal entities in the form of bearer shares is not permitted in France.

In addition, financial institutions and *bureaux de change* are forbidden from keeping anonymous books and accounts.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

There is an obligation for persons other than those mentioned in article L. 561-2 of the Monetary and Financial Code, and who, in the course of their professional activities, carry out, control or advise on transactions involving movements of capital, to report to the public prosecutor transactions on funds, which they know are the proceeds of an offence carrying a prison sentence of more than one year or linked to financing terrorism.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Article L. 561-10 of the Monetary and Financial Code provides for additional AML requirements listed under article R. 561-20, III of the same code where a transaction involves natural or legal persons, including their subsidiaries or establishments, domiciled, registered or established in a State or territory appearing on the lists by the FATF or the European Commission, among those whose legislation or practices impede the fight against money laundering and terrorism financing.

Articles L. 561-10 and R. 561-20, II also provides for additional AML requirements where the customer is a politically exposed person (PPE). The AMF has published guidelines on the identification of PPEs for financial institutions.

Prior to Decree n° 2018-284, and according to article R. 561-18, a PPE was a person residing in a country other than France and subject to increased risks because of the person's political, judicial or administrative role or function, either current or in the previous year. A PPE is now defined as any person having had such political, administrative, judicial duties, irrespective of their country of residence, be it in France or abroad.

Customers that are family members, beneficial owners, or close business partners of PPEs also require increased scrutiny on AML.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Amendments to the fourth EU Directive against money laundering, conveniently referred to as the fifth EU Directive (Directive (EU) 2018/243), which came into force on July 9, 2018, have now to be transposed in France as in all Member States by January 10, 2020.

These amendments notably require tax-related service providers, art traders under specific conditions, and new financial businesses, including, cryptocurrency trading platforms, to abide by AML requirements. The fifth Directive also provides for increased cooperation between European Financial Intelligence Units, as well as for publicly accessible beneficial ownership registries.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The most recent report on France's anti-money laundering regime by the FATF pointed out a significant lack of regulation, supervision and monitoring of non-financial institutions and professional activities with regard to AML requirements.

The FATF identified several factors including difficulties in assessing the effectiveness of inspections in overseas territories, and a lack of technical and human resources in self-regulated organisations for enforcing compliance with AML requirements.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

France's anti-money laundering regime has been evaluated several times by the Financial Action Task Force. The last FATF report (Mutual Evaluation Report) was published on February 25, 2011.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Laws and regulations are available on the internet, although not necessarily in English, on the *Legifrance* website. Translations in English of the Monetary and Financial Code, Criminal Code and Code of Criminal Procedure are available. However, most translations are not up-to-date with the most recent changes in legislation. TRACFIN also offers guidance on its dedicated website, but not in English.

Extensive information on anti-money laundering measures in France can be obtained in English on the websites of *France Diplomatie*, the Banking Commission and the *Autorité des Marchés Financiers*.

Acknowledgment

The author would like to acknowledge the assistance of Caroline Goussé, member of the Paris and New York Bar, in the preparation of this chapter.

Stéphane Bonifassi

BONIFASSI Avocats
34 boulevard Haussmann
75009 Paris
France

Tel: +33 1 82 28 10 81
Email: s.bonifassi@bonifassi-avocats.com
URL: www.bonifassi-avocats.com/en

Stéphane Bonifassi, founder of Bonifassi Avocats in Paris, concentrates his practice on complex, international financial crimes. With more than 26 years' experience in the criminal courts, he has honed an approach that combines targeted investigative and litigation tactics to locate and recover stolen or hidden assets, as well as defend those accused of committing financial crimes. Bonifassi has been recognised as the "dean of the Parisian Bar" for his mastery of all aspects of the French legal system, paired with his ability to manage corresponding proceedings abroad.

BONIFASSI
AVOCATS

BONIFASSI Avocats specialises in international litigation, involving complex financial crimes, with a focus on fraud, money laundering, corruption and asset recovery.

This practice area requires proven trial experience, demonstrated investigative tactics, a sophisticated understanding of litigation tools and proceedings, and an intrinsic familiarity with mutual legal assistance issues.

While excelling in these areas, our partner and associates also bring a depth of talent, passion and international experience in:

- Enforcement of foreign judgments and arbitral awards.
- Transnational enforcement of confiscation orders, insolvency judgments and receiverships.
- Criminal law and procedure, in an international context.

As a boutique firm, we offer our clients a commitment to personal attention characterised by accessibility, responsiveness and efficiency. Yet with our technical expertise and focus in the areas of fraud, asset recovery, corruption and white-collar crime, our experience and international reach equal that of larger law firms.

Germany

Dr. Dirk Seiler

Herbert Smith Freehills Germany LLP

Enno Appel

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In Germany money laundering is prosecuted at a regional level by the respective state prosecutors' offices. Investigations are conducted by the State Office of Criminal Investigations (*Landeskriminalamt*) and local police.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Criminal money laundering pursuant to Section 261 of the German Criminal Code (StGB) entails the following elements: (1) money or other assets are the proceeds of a predicate offence; (2) the proceeds were intentionally concealed, disguised, procured (for himself or a third party), used (for himself or others) by the offender or their origin, or tracing or confiscation was thwarted or endangered by the offender; and (3) the offender is aware that the assets are the proceeds of a predicate offence and acts with intent in this respect. It is also a criminal offence if an offender acts merely grossly negligent in that he fails to acknowledge criminal origin. In the latter case, the maximum sentence is reduced.

Predicate offences (attempt suffices) are (Section 261 (1) StGB):

- severe crimes with a minimum sentence of at least one years' imprisonment (e.g. robbery);
- active and passive bribery of public officials; drug-related offences; commercial, forceful or organised evasion of customs and violation of customs provisions and smuggling/procuring such goods; and
- subversive acts of violence capable of threatening the existence or the security of the state/international institution; formation of criminal/terrorist associations as well as committing of criminal offences as a member of a criminal/terrorist association, if not already a predicate offence.

The following offences qualify as predicate offences only if committed in a continued manner as part of commercial activity or within an organised association:

- tax evasion; forgery of credit cards and cheque cards; pimping; human trafficking; exploitation of another person through labour (e.g. slavery); theft, concealment, extortion; receiving stolen goods; fraud and specific types of it; embezzlement; forgery of documents and related offences, unauthorised organisation of gaming; unauthorised dealing with toxic waste, or radioactive or other hazardous substances; commercial active and passive bribery illegal smuggling of foreigners; inciting improper applications for asylum; insider trading; offences related to intellectual property, e.g., copyright infringement.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In general, German criminal law is applicable if the crime was committed in Germany (Sections 3, 9 StGB) or on an aircraft/ship operating under the German flag (Section 4, 9 StGB). This includes every place where the offender acted or in which the result – if it is an element of the offence – occurs.

Crimes committed abroad are only applicable if: (1) the victim is a German citizen (Sections 7 (1) StGB) and the offence is also punishable in the foreign country or if the crime is committed outside any jurisdiction (e.g. at sea); (2) the offender is a German citizen (Section 7 (2) No 1StGB); (3) the offender is captured in Germany and cannot be extradited (Section 7 (2) No 2 StGB); or (4) the crime concerns internationally protected interests as enumerated in Section 6 StGB such as drug trading.

The money laundering offence has a particularly extensive extraterritorial reach because it applies if the predicate offence was committed abroad, is punishable in that country and if the proceeds are "laundered" in Germany (Section 261 (8) No. 8 StGB).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Regional state prosecutors are responsible for investigating and prosecuting money laundering criminal offences. (See question 1.1 above.)

1.5 Is there corporate criminal liability or only liability for natural persons?

German criminal law only applies to natural persons. However, there are provisions in the Administrative Offences Act (OWiG) imposing fines upon companies if criminal offences have been committed by executive employees, and/or if the executive employees have failed to adhere to their supervisory obligations relating to the prevention of criminal offences (Section 30, 130 OWiG).

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Money Laundering is punishable by imprisonment of between three months to five years. The penalty increases to six months to 10 years if the crime was committed on a commercial or organised basis in a continued manner. A reduction applies if committed with gross negligence.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is five years after the offence has ended.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

The federal law is enforced by regional state prosecutors. There are no parallel state/provincial offences in Germany.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Sections 73 *et seq.* StGB apply to all criminal offences including money laundering/predicate offences. It is the court in the relevant district which issues the confiscation order.

Subject to confiscation are assets which have been obtained by or used for the criminal offence, i.e. proceeds of (Section 73 StGB), instrumentalities and objects which are part of the crime (Sections 74/74b, 261 (7) StGB):

- "Proceeds" encompasses any measurable economic advantage obtained because of the offence such as: movable items; real estate and legal rights; claims; and saved expenses. Foreign assets can also be subject to confiscation.
- "Benefits derived from proceeds", i.e. indirect proceeds, e.g., objects received in exchange for the proceeds including income and profits can be confiscated.
- "Instrumentalities" are assets, products of the crime or assets intended for its commission. They must be owned by the offender at the time of the court order or if the relevant assets are dangerous.
- "Objects of the crime" are assets which are part of the crime and necessary to commit it. They must be owned by the offender.

Confiscation may also be ordered if the origin of the assets cannot be traced back to a specific, convicted crime but which are certainly the proceeds of crime (Section 73a StGB).

Third parties may be subject to confiscation if they obtained the incriminated asset for free, if they should have known they are the proceeds of crime or if the offender acted for them (Section 73b/74a StGB).

The court may also order that the value of the obtained assets will be confiscated if confiscation of the actual asset is not possible (Section 73c StGB).

Assets of a company can be confiscated if the crimes were committed by its representative bodies or legal representatives (Section 74e StGB).

In general, confiscation can only be ordered on the basis of a conviction. There are, however, exceptions to this rule:

- Proceeds, instrumentalities and objects can be confiscated if no one can be convicted and prosecuted for the crime (Section 76a StGB).
- There are provisional measures in German civil law which allow for the provisional seizure of assets, but only for the purpose of ensuring that they are not divested of until the underlying dispute has been resolved and to secure a later enforcement (Sections 916 *et seq.*).

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

In the past years, directors, officers and employees of financial institutions have been sentenced in Germany. However, most of these criminal proceedings are resolved without public prosecution and public hearings. Therefore, only limited information is publicly available.

In 2018, Frankfurt prosecutors initiated investigations against employees of a German Bank concerning alleged aiding and abetting of money laundering.

In 2015, Frankfurt prosecutors investigated five employees of a German Bank in connection with the carbon trading scandal. The individuals were accused of conspiring to evade tax of approx. EUR 220 million in the trading of carbon emission certificates. Some of the involved employees were AML officers. The bank was not convicted as no corporate criminal liability exists in Germany. However, the bank was fined for the lack of adequate procedures to prevent money laundering in the amount of EUR 40 million.

In 2011, charges were pressed against four employees of another German Bank for money laundering in a continued manner as part of commercial activity and within an organised association. The employees allegedly helped to channel approx. USD 113 million from Russia through Europe and Bermuda.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Section 153 German Code of Criminal Procedure (StPO) stipulates that prosecution may be ceased if the crime is minor and if the public does not have any interest in prosecution. The cease decision may be combined with an order to pay a fine. The cease decision is not public.

There is the possibility to enter into a deal during court proceedings if all participants agree and only with respect to the extent of the sentence (Section 257c StPO). The details of the deal are not public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The supervising and monitoring authorities are for:

- banks and other financial institutions: Federal Financial Supervisory Authority ("*BaFin*");
- lawyers and legal advisors: local bar/professional associations;

- notaries: president of the regional court in the relevant district;
- auditors, registered accountants and tax advisors/agents: chamber of the profession, for example, the Chamber of Tax Advisors; and
- casinos, gaming companies and commercial traders of goods (*Güterhändler*): the respective supervisory authority of the federal states.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Lawyers, legal advisors, notaries, auditors, registered accountants and tax advisors/agents are regulated by self-regulatory bodies. These might impose binding money laundering requirements on a secondary level.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, for lawyers, notaries, auditors, registered accountants, tax advisers and agents the respective self-regulated bodies are responsible for compliance and enforcement.

2.4 Are there requirements only at national level?

The money laundering requirements are entirely codified in the federal Anti-Money Laundering Act (GWG) and partially in the Banking Act (KWG).

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The German regulator BaFin has published new interpretative and application notes (*Auslegungs- und Anwendungshinweise*) for the implementation of the due diligence and internal safeguard measures to prevent money laundering. See also question 2.1 above.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The FIU (*Zentralstelle für Finanztransaktionsuntersuchungen*) has been established at the General Directorate of Customs (*Generalzolldirektion*). The FIU's core responsibility is to analyse and assess filed suspicious activity reports. In this regard, it also has unlimited access to data of prosecution offices, public financial agencies and public administrative agencies. Furthermore, it has the power to halt suspicious transactions for up to one month. The FIU will decide whether the case needs to be forwarded to the prosecution offices. The FIU also coordinates international collaboration with foreign authorities.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The limitation period for prosecuting money laundering-related administrative offences is three years (Section 31 OWiG).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Section 56 (2), (3) GWG set out that for particularly grave and systematic offences and for specific obliged entities the maximum fine is between EUR 1 to 5 million or 10 per cent of the gross income of the entity in the preceding year, depending on which figure is higher. In all other cases, a fine of up to EUR 100,000 may be imposed.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Depending on the gravity of the offence, it is possible that the responsible authority revokes required licences on account of permanent violations of anti-money laundering provision (e.g. Section 35 (2) No. 6 KWG and Section 51 (5) GWG).

Furthermore, for financial institutions BaFin may demand the dismissal of the managers responsible and may also prohibit these managers from carrying out their activities at institutions organised in the form of a legal person (Section 36 (1) and (2) KWG).

Furthermore, the competent authority has the power to order specific compliance undertakings and remedial measures (Section 51 (2) GWG).

Financial penalties can also be imposed on financial institution directors, officers and employees in addition to the financial institution.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

In addition to the fines described above (see question 2.8 above), the criminal offences (see question 1.2 above) and fines for the failure to adhere to supervisory obligations (see question 1.5 above), the KWG contains criminal sanctions for CEOs of financial institutions for specific violations of their organisational duties, *inter alia*, the duty to implement risk management processes and procedures (Section 54a KWG).

The competent authority may also initiate audits at the respective institution and may – if the specific legal requirements are met – impose certain measures to remedy shortcomings and mitigate risks (e.g. Section 44 *et. seq.* KWG).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

In general, administrative offences in the sense of OWiG follow the below process:

Prosecution is initiated by the responsible public authority, possibly together with the criminal prosecutor or the criminal court; it is required that the offender is given the opportunity to respond to the allegations. In order to challenge the measures taken by the public authority, the addressee of these may request a court decision (Section 62 OWiG).

If the offence is minor, the public authority can impose a warning fine of up to EUR 50. If the offence also qualifies as a criminal offence, the prosecution office will initiate criminal proceedings.

In all other cases the responsible authority will issue a notice specifying the sanction (*Bußgeldbescheid*). This notice can be challenged within two weeks, and if this challenge is admissible court proceedings are commenced. The court will decide on the lawfulness of the notice and the court decision can be appealed.

The public authority may also order confiscation. After the notice has become legally valid it may be enforced subject to the provisions of the Law on Administrative Enforcement.

In the past not all actions were publicly available. Since June 2017, legally valid measures and monetary sanctions are made public on the website of the responsible public authority (Section 57 GWG).

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The obliged entities are enumerated in Section 2 GWG and include: credit institutions; comparable financial services entities; institutions which offer payment services and electronic money; agencies which offer similar services or independent entities which offer the services as agent insurance companies, insurance agents, capital management companies, lawyers, patent lawyers, notaries, legal advisors, auditors entities which provide trust services, brokers; gambling companies; and companies which commercially trade goods.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Cryptocurrencies are not regulated explicitly by law, and, according to BaFin, the mere creation and use of virtual currencies is not subject to permission. However, the BaFin qualifies crypto currencies as units of account (*Rechnungseinheiten*) that are regulated by law as a part of "financial instruments". If the usage of cryptocurrencies meets all characteristics of regulated transactions in financial instruments, it qualifies the offering company as a credit institution, comparable financial services entity or an institution which offers payment services for which the anti-money laundering requirements apply (see question 3.1 above).

Therefore, all companies in the cryptocurrency industry have to examine if their own business practices affect any special legal regulation regarding financial service transactions. The relevant catalogue of businesses can be found in Section 1 KWG and Section 1 of the Payment Services Supervision Act (ZAG).

If, for instance, a company sells cryptocurrencies on commission or on behalf of their clients, it qualifies as a financial commission business under Section 1 Subsection 1 Nr. 4 KWG and, therefore, is an obliged entity under Section 2 GWG.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All obliged entities are required to implement procedures comprising, *inter alia*, an efficient risk management system under the GWG which sufficiently ensures that the due diligence, reporting and record-keeping obligations are met and regularly monitored and that necessary suspicious activity reports are filed.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

General due diligence obligations are triggered by transactions outside of an existing business relationship if they are cash transactions and exceed EUR 1,000, or for all other transactions if they exceed EUR 15,000.

For specific obliged entities, the thresholds deviate from the above: (1) for gambling companies EUR 2,000; (2) for companies commercially trading goods the obligations are triggered in suspicious circumstances, or if they accept cash of EUR 10,000 and above; and (3) for insurance agents if they receive more than EUR 15,000 in cash within a year.

Meeting these thresholds does, however, not necessarily mean that the reporting obligation in Section 43 GWG is triggered. The reporting obligation does not specify the value of a transaction as a triggering factor. The provision vaguely refers to circumstances which appear suspicious.

Financial institutions have the specific obligation to retain records regarding large and complex transactions which is part of their customer due diligence obligation, and which they must do regardless of the client's risk qualification. The records must sufficiently demonstrate that the obligation was complied with (Section 25 h (3) KWG).

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, there are no such requirements other than in cross-border transactions (see question 3.6).

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

For cross-border transactions, the Foreign Trade and Payments Act (AWG) in conjunction with the Foreign and Trade and Payments Regulation (AWV) applies which entails reporting obligations which have to be filed electronically to the Federal Bank of Germany (*Bundesbank*) subject to certain deadlines. The Federal Bank may issue exemptions to these obligations on a case-by-case basis.

Payments exceeding EUR 12,500 must be reported (Section 67 AWV): all residents in Germany including companies will have to report to the Federal Bank if they receive or make payments exceeding EUR 12,500 (or the equivalent in foreign currency) from

a non-German resident or from a German resident but for the account of a non-German resident (incoming and outgoing payments). The obligation does not apply to cash physically carried abroad. The Federal Bank provides the relevant forms for the reporting. The term 'resident' does not refer to nationality but rather the place of habitual residence which means that if a German citizen has been living abroad for more than one year he will be considered a non-resident. There are exemptions to this, *inter alia*, payments received/made for exported/imported goods, payments and repayments of loans and deposits with an original maturity of up to 12 months and payments made by financial institutions within long-term credit transactions with non-residents.

Resident banks and similar financial service entities have an additional obligation with respect to payments exceeding EUR 12,500 if those relate to the sale of stocks, derivatives to/from foreigners or encashing of such; payment of interest and dividends on resident stocks to/from foreigners, or payments related to interests (Section 70 AWV).

Other reporting obligations relate to assets exceeding a certain value if held by a resident abroad and such assets held by a non-resident in Germany (Section 65 AWV), claims and debts relating to funds of resident financial institutions exceeding EUR 5 million, investment stock companies and capital management companies (Section 66 AWV) and claims and debts exceeding EUR 500 million resulting from financial relationships with foreigners of the same entities (Section 66 AWV). A violation of these provisions may result in an administrative fine (Section 81 AWV).

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

General due diligence obligations have to be performed regardless of the risk classification and are triggered when a business relationship is established and for one-off transactions exceeding the thresholds (EUR 1,000 in very specific cases and usually EUR 15,000) and if there are suspicious indications.

The obligations are: (1) identification of the client by obtaining the information specified in Section 11 GWG and verification of this information through, *inter alia*, documents specified in Section 12 GWG; (2) identification and verification of the person acting on behalf of the client; (3) clarification of whether the client acts for a beneficial owner and if so, identification of the beneficial owner and verification of the obtained information; and (4) obligations to conduct a risk analysis and implement a risk management system including business and customer related internal safeguards such as, e.g., internal policies, the appointment of an anti-money laundering officer.

When assessing the customer-related risk, the entities must at least consider the purpose of the business relationship, the amount of the assets and the regularity and duration of the business relationship.

Relationships with high-risk clients additionally trigger enhanced due diligence obligations, *inter alia*, obtaining information on the source of wealth, enhanced monitoring and obtaining management approval. A high risk exists if one of the following applies: the client or beneficial owner is a politically exposed person, a family member or closely related person; or a transaction is unusual with respect to complexity, size or is conducted for no economic or rightful purpose (Section 15 (3)). Annex 2 of the GWG contains additional high-risk indicators.

Correspondent relationships between financial institutions and comparable financial entities located in a third-party state are considered and will trigger obligations specific to correspondent relationships (Section 15 (6) GWG).

If the client is categorised low-risk the entity is, *inter alia*, allowed to reduce the intensity of the measures. They may, in particular, deviate from the specific verification requirements. Annex 1 contains specific low-risk indications in a non-exhaustive list (Section 14 GWG).

Parent companies which have subsidiaries abroad are required to ensure that such processes and safeguards exist throughout their group (Section 9 GWG).

For financial institutions, the described obligations apply and are supplemented by the KWG which contains more specific requirements with respect to, e.g., required internal safeguards (Section 25 *et. seq.* KWG).

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

For credit institutions, business relationships with shell banks are prohibited pursuant to Section 25m KWG.

3.9 What is the criteria for reporting suspicious activity?

Pursuant to Section 43 GWG, a report has to be filed without undue delay if the facts indicate that the assets which are connected to the business relationship, a specific transaction, or a brokerage relates to a crime which is a predicate offence to money laundering, to terrorist financing, or if there are indications that the client failed to disclose beneficial ownership.

Lawyers, notaries, patent lawyers, auditors, tax advisors and similar professions might be exempted from suspicious activity reporting if the respective circumstances are covered by their professional privilege.

According to Section 261 (9) StGB, an offender is exempt from any penalty if he or she either reports the crime voluntarily to the responsible authority or ensures seizure of the respective assets. The suspicious activity report may qualify as such a voluntary report and may, thus, exclude a criminal penalty.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

In 2017, Germany established a "Transparency Registry" and legal entities, shareholders and trustees are required to disclose information on their beneficial ownership to the responsible authority.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Payment orders are required to include sufficient information about the originator (name or customer ID) and an account number to which

the transfer is made. However, the bank is not required to check whether the name on the payment order matches the account number.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Yes, it is permitted; however, it will be deemed a risk-enhancing factor.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

The GWG provisions apply to a variety of non-financial institutions.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

The GWG also applies to persons commercially trading with goods (see question 3.1 above), but there are no specific anti-money laundering requirements for free trade zones.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

There are ongoing discussions in Germany as to whether there is a need for corporate criminal liability. Furthermore, there are preparations for a new directive which extends the anti-money laundering regime explicitly to virtual currencies.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

It has been pointed out in the 3rd Follow-up Report of the FATF in 2014 that Germany lacks criminal liability for self-laundering. Recommendations that had been made in the previous report, such as an incomplete list of predicate offences, were addressed by the German legislator according to the FATF.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes, see question 4.2. The report is titled "Mutual Evaluation of Germany: 3rd Follow-up Report" and can accessed through the following link: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FUR-Germany-2014.pdf.

The next evaluation is scheduled for 2020.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The most relevant texts are available on the website of BaFin. For example, you can find an English translation of the GWG here: https://www.bafin.de/EN/RechtRegelungen/Rechtsgrundlagen/Gesetze/gesetze_artikel_en.html?nn=8356586.

Dr. Dirk Seiler

Herbert Smith Freehills Germany LLP
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Tel: +49 69 2222 82535
Email: dirk.seiler@hsf.com
URL: www.herbertsmithfreehills.com

Dr. Dirk Seiler is a partner in the Dispute Resolution/Corporate Crime and Investigations practice group at our Frankfurt office. Dr. Seiler has advised national and international companies on investigating and handling complex cases of white-collar crime/compliance since 2003. A focal point of his work at the interface between civil and criminal law involves cases of corruption, embezzlement, misappropriation and fraud.

In recent years, Dr. Seiler has been involved in several major cases, investigating facts and enforcing eight-figure claims both in and out of court. Cases attracting considerable public attention included the civil and criminal law representation of injured companies in the waste scandal in Cologne and Bonn, the case involving the money transport company Heros, and the Ikea and Ford cases. In the field of preventive compliance advice, Dr. Seiler has been representing high-profile companies from various industries for a number of years.

Enno Appel

Herbert Smith Freehills Germany LLP
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Tel: +49 69 2222 82516
Email: enno.appel@hsf.com
URL: www.herbertsmithfreehills.com

Enno Appel is a senior associate in our Dispute Resolution/Corporate Crime and Investigations practice group at our Frankfurt office. He specialises in advising and representing national and international companies in the fields of compliance/white-collar crime and the associated internal investigations and lawsuits. Enno regularly advises international banks and other clients on regulatory obligations under the anti-money laundering (AML) and anti-bribery and corruption (ABC) laws and in cases of fraud and embezzlement. Enno has been recognised as one of the next generation's lawyers in the area of Internal Investigations.

HERBERT SMITH FREEHILLS

Our lawyers in Berlin, Düsseldorf and Frankfurt provide local and international clients with leading expertise in corporate/M&A, dispute resolution, finance, capital markets, real estate, competition/regulatory and employment matters, general commercial issues as well as advice on compliance matters, corporate crimes and investigations.

With a major focus on cross-border work we operate seamlessly within our global network to provide clients with the highest level of service. Through continuous effort the German practice has grown significantly over the past years.

Chapter 13

Greece

Ilias Anagnostopoulos

Alexandros Tsagkalidis

Anagnostopoulos

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Criminal law enforcement lies with the Prosecutor's Office. All enforcement agencies (the Hellenic FIU, the Financial and Economic Crime Unit, the Capital Market Commission, etc.) forward their reports with findings and gathered information of suspicious activities to the Prosecutor's Office. As a general rule, enforcement agencies have the power to collect information, report their findings and proceed with necessary investigative acts. However, everything is coordinated by the prosecutor. The prosecutor evaluates the material in hand and initiates whatever proceedings are necessary.

In cases of emergency, certain powers are given to the Hellenic FIU for securing traced assets (proceeds of crime or related to money laundering activities) whereby the head of the Hellenic FIU issues a freezing order in order to prevent loss or further concealment of property. These orders are also reviewed by the prosecutor and, if necessary, following a request by the interested party, by a judicial council.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Law 4557/2018 is the main law against money laundering. According to article 2, the act of money laundering is described as follows:

- knowingly converting and transferring property assets that are the proceeds of a crime, or participation in such an act for the purposes of concealing the illegal sources of the assets, or aiding anyone involved in said acts in order to assist in avoiding legal sanctions;
- concealing and covering up the truth, by any means, in relation to the source, movement, disposal, place of acquiring assets or asset-related rights, knowledge that a property is associated with the proceeds of criminal acts or participation in criminal activities;
- acquiring, possessing, managing or using any asset with the knowledge that at the time of possession, management, etc., such property asset was the proceeds of a criminal activity;
- using the financial sector by depositing or transferring proceeds of criminal activities for the purposes of making it appear as though they have legitimate sources;
- forming a group or organisation for the purposes of committing one or more of the above-mentioned actions; and
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in above points.

Furthermore, it is required that the natural person acts in the knowledge (*dolus directus*) of the source of the assets and for the purposes of concealing or covering up their true origin. Therefore, there is no room for negligently committing an act of money laundering.

Article 4 of Law 4557/2018 contains a list of predicate offences of money laundering. The list contains all forms of classic corruption and property-related offences, namely, bribing of domestic public officials, bribing of foreign officials or EU officials, fraud, tax evasion and tax fraud, capital market offences, including offences related to insider trading, antiquities trafficking, environmental offences, drug trafficking, people trafficking, organised crime and terrorism financing. Tax evasion is listed as a predicate offence as well.

Moreover, the list contains a general provision according to which any offence that results in asset or property profits and is punishable by law with a minimum of six months' imprisonment may be considered a predicate offence. In other words, all criminal activities that can produce money or asset gains or profits may be considered as predicate offences. This provision makes the list of predicate offences non-exhaustive, since it leaves room for any type of criminal behaviour that results in profit, even if it is of lesser to medium importance (as it includes misdemeanours punishable by imprisonment of a few months).

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In principle, AML legislation and regulations apply to individuals and institutions based in Greece or are active within the Greek territory. Greek money laundering laws are applicable to Greek citizens and non-citizens even if the predicate offence has been committed abroad, as long as it constitutes an offence in accordance with the laws of the foreign country and provided that the laundering act was committed within Greek territory. Moreover, Greek citizens may be prosecuted for laundering acts committed in a foreign country, provided that the dual criminality requirement is fulfilled.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Please see the answer to question 1.1.

1.5 Is there corporate criminal liability or only liability for natural persons?

Criminal liability lies with a natural person, and consequently there is no criminal liability in its traditional sense regarding a business or entity. For the purposes of applying legal provisions related to corporate practices and activities, there are provisions for liability in the form of administrative penalties and fines, depending on the seriousness of the act, size of the business, etc.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalties are as follows:

Individuals: Incarceration of up to 20 years and a monetary sentence of up to €2,000,000.

Legal entities: An administrative fine ranging from €50,000 up to €10 million, which is always applicable, and:

i) suspension of activities temporarily or permanently;

ii) prohibition of certain activities to be performed by the company, or establishment of branches; and

iii) a ban from public tenders, subsidies, etc.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is 15 years from the time the offence was committed. This period is suspended for five years when the case file is forwarded to a trial-hearing.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

No, there are no parallel state or provincial criminal offences.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Agencies such as the SDOE and the FIU, along with the judicial authorities (the investigating judge and the prosecutor during the main investigation, or the judicial council during the preliminary inquiry) are responsible for tracing and freezing assets that are allegedly the proceeds of crime. Confiscation of such assets can solely be ordered by the court that tries the case if the defendant is found guilty of committing such crimes.

Assets derived from a predicate offence or from money laundering or acquired directly or indirectly from the proceeds of such offences, or the means that were used or were going to be used for committing these offences shall be seized and, if there is no legal basis for returning them to the owner according to article 310, paragraph 2 and article 373 of the Greek Code of Criminal Procedure, shall be compulsorily confiscated by virtue of the court's judgment.

Confiscation shall be imposed even if the assets or means belong to a third person, provided that such person was aware of the predicate offence or the offences referred to in article 2 of Law 4557/2018 at the time of their acquisition. Where the assets or proceeds above no longer exist or have not been found or cannot be seized, assets of a value equal to those assets or proceeds as at the time of the court's judgment, shall be seized and confiscated. Their value shall be determined by the court. The court may also impose a pecuniary penalty up to the value of those assets or proceeds if it rules that there are no additional assets to be confiscated or the existing assets fall short of the value of those assets or proceeds.

Furthermore, according to the recently amended article 76 of the Greek Criminal Code, in case of a guilty verdict, all assets derived from the commission of a felony or from a serious misdemeanour, as well as all assets acquired (directly or indirectly) from the proceeds of such offences, are subject to confiscation. In case these assets have been 'mixed' with lawfully obtained assets, confiscation shall apply to assets up to the value of the assets that derived from the offence. Confiscation of assets is not enforced, when it is deemed disproportionate (i.e., it is highly likely that it will cause a serious and irreparable damage to the defendant's livelihood or to his family).

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Financial institutions have been subject to administrative sanctions; appeals against such sanctions are pending before the administrative courts.

Charges against individuals are currently pending before criminal courts.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The Greek Criminal Procedure Code does not provide for extra-judicial settlement of criminal actions. Full compensation of the victim for financial losses, etc., may be the basis for leniency or (at an early stage of the proceedings) for the termination of criminal proceedings.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Enforcement and supervision of covered institutions and persons is done through government entities and quasi-governmental entities which are competent in their respective field. Banking, financial and insurance institutions are supervised by the Bank of Greece. Corporations listed in the stock market are regulated by the Hellenic Capital Market Commission. Other businesses are regulated by the competent department of the relevant ministry (e.g. Ministry of

Commerce), lawyers and notaries by the Ministry of Justice, etc. (a comprehensive list is provided for in article 6 of Law 4557/2018). All regulatory agencies and institutions liaise with the central regulating authority, which is the Ministry of Finance.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

For each category of covered institution anti-money laundering regulations and guidelines are issued by the supervising administrative authorities (e.g. decisions issued by the Bank of Greece).

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, they have powers to impose sanctions of an administrative nature.

2.4 Are there requirements only at national level?

Greece is a member of the Financial Action Task Force (FATF), the FIU-Net and the Egmont Group through the Hellenic FIU. It is also a member of the EU and the Council of Europe and cooperates with all major international bodies and organisations related to combatting money laundering. In this context, international money laundering standards and requirements are implemented at a national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see the answers to questions 2.1 and 2.2.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Hellenic FIU is the competent authority to: collect information from reports filed on suspicious transactions or any other source; make use of information communicated by foreign authorities; release guidelines to natural persons or businesses covered by Law 4557/2018 on applying the law; and cooperate and exchange information with international organisations with similar powers. The Hellenic FIU is a member of the FIU-Net and the Egmont Group and files its annual report with the Commission on Transparency of the Hellenic Parliament, the Ministry of Finance, the Ministry of Justice and the Ministry of Citizen Protection.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Limitation periods vary depending on the classification of the act as misdemeanour or felony. For misdemeanours (imprisonment for up to five years), the limitation period is five years between the act and indictment. After indictment, the limitation period is suspended for three more years. For felonies (imprisonment for between five and 20 years), the limitation period is 15 years between the act and indictment. After indictment the limitation is suspended for an additional five years.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

All covered institutions and their employees have three basic obligations (articles 22 and 27 of Law 4557/2018): to report immediately to the FIU on suspecting that an act of money laundering has been committed or is about to be committed; to offer immediately all information requested by the FIU or other supervising authorities; and not to inform the client or any third party either that they have filed a report of suspicious transactions or they have received a request to give information to any authority. Breach of the latter prohibition is punishable by imprisonment for three months (minimum) to five years and a fine.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

As per the provisions of article 46 of Law 4557/2018, failure to comply with anti-money laundering regulations may also lead to:

- removal of the directors, the managing director, management officers of the legal entity or other employees for a specific time period and prohibition of assuming other important duties;
- prohibition from carrying out certain activities, establishing new branches in Greece or abroad or increasing its share capital; and
- in case of serious and/or repeated violations, final or provisional withdrawal or suspension of authorisation of the corporation for a specific time period or prohibition to carry out its business.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Penalties for breaching anti-money laundering obligations are mainly administrative. Breach of confidentiality with regard to the reporting of suspicious transactions is punishable by imprisonment for three months (minimum) to five years and a fine (article 27 of Law 4557/2018).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

In most cases, the supervising authorities are notified by the prosecutorial and police authorities. However, no sanction shall be imposed without prior summons of the legal representatives of the legal entity to provide their views. The summons shall be served 10 working days before the day of the hearing at the latest. The administrative decisions imposing penalties on legal entities may be challenged before the competent administrative courts.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

As per article 5 of Law 4557/2018, the following legal/natural persons are subject to anti-money laundering requirements: a) credit institutions; b) financial institutions; c) venture capital companies; d) companies providing business capital; e) chartered accountants, audit firms, independent accountants and private auditors; f) tax consultants and tax consulting firms; g) real estate agents and related firms; h) casino enterprises and casinos operating on ships flying the Greek flag, as well as public or private sector enterprises, organisations and other bodies that organise and/or conduct gambling and related agencies and agents; i) auction houses; j) dealers in high-value goods, only to the extent that payments are made in cash in an amount of €10,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked; k) auctioneers; l) pawnbrokers; m) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their clients in any financial or real estate transaction, or by assisting in the planning and execution of transactions for the client concerning the i) buying and selling of real property or business entities, ii) managing of client money, securities or other assets, iii) opening or management of bank, savings or securities accounts, iv) organisation of contributions necessary for the creation, operation or management of companies, or v) creation, operation or management of trusts, companies or similar structures; and n) natural or legal persons providing services to companies and trusts (trust and company service providers) which by way of business provide any of the following services to third parties:

- forming companies or other legal persons;
- acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons or arrangements;
- providing a registered office, business address, correspondence or administrative address and any other related services for a company, a partnership or any other legal person or arrangement;
- acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement; or
- acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

As per article 3 of Law 4557/2018, electronic and digital assets are considered "property" for the purposes of the said law. Therefore, anti-money laundering legislation is applicable for all transactions involving cryptocurrency.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All covered institutions and persons need to implement AML compliance programmes, usually following guidelines and regulations of the competent supervising authorities. Naturally, covered institutions more vulnerable to money laundering activities (e.g., banks, financial institutions, insurance institutions) have more comprehensive and detailed AML compliance programmes, especially because these institutions are under strict supervision and regulation. The minimum elements of an AML compliance programme (minimum may vary depending on the nature of the covered institution or person) are related to validating the transaction as much as possible and identifying transacting parties in order to eliminate suspicions of questionable conduct or unknown, untraceable origins of assets.

However, even natural persons (e.g., lawyers and notaries) have to meet the standards set by the competent supervising authority (Ministry of Justice, bar associations and notary associations) in relation to the management of trusts or transactions on behalf of the client.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Suspicious activity is that which indicates that a money laundering offence is committed or has been attempted, or where there is sufficient indication that the transacting party is involved in other criminal activity (predicate offences). This assessment is made in view of the characteristics of the transaction, the background of the client (financial, professional, etc.) and a history of the client's transactions. Diligence rules apply to transactions over €15,000. Suspicious transactions must be reported immediately to the Hellenic FIU along with all relevant information to be requested by the FIU.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

The Ministry of Finance has issued a series of circulars in respect of the application of anti-money laundering laws and regulations and bookkeeping obligations, whereby auditors and accountants are given specific guidelines to report any transaction that causes any suspicion of being related to a criminal act (even if it is a simple or general suspicion without need for proof) to the Hellenic FIU.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Cross-border transactions which take place within covered institutions (e.g. money remittances to or from bank institutions in Greece) are subject to the same anti-money laundering requirements as local transactions.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Law 4557/2018 outlines a complex set of diligence rules for the covered persons to follow, applicable to new clients, existing clients, high-risk individuals, politically exposed persons, transactions on new financial products, transactions executed without the client's physical presence, etc.

Rules of diligence apply when the covered institutions enter a business agreement with the client, when they process occasional transactions of more than €15,000, when there is suspicion that an offence has been committed or is about to be committed and when there is doubt about the accuracy of information obtained for the purposes of confirming and verifying the identity of the client or another person acting on behalf of the client.

According to the rules of ordinary diligence, covered institutions must take the necessary action to verify the identity of the client and the identity of the beneficial owner in relation to the executed transaction, and to gather information on the economic background of the client in order to check whether a transaction is in accordance with this background, etc.

The means that a financial institution uses to make the necessary cross-references must be appropriate (according to the Law's description) in order to identify the individuals, the transaction and the beneficiary owner.

As regards the beneficiary ownership, there is a description given by the Law (article 4, paragraph 16) and is generally the person in favour of whom the transaction is executed or the person in control of an entity or a group of entities (directly or indirectly) in favour of which the transaction is executed. The main concept is to find who benefits eventually from the transaction.

Covered institutions must conduct risk-based analysis where a transaction is related to politically exposed persons (e.g., members of the government, members of parliament, heads of state, directors of central banks, ambassadors, high-ranking members of the judiciary). Stricter rules of diligence also apply to transactions without the presence of the client, cross-border transactions, and transactions related to new financial products or with the use of new technology. Covered institutions are obliged to take additional measures to avoid the execution of a suspicious transaction and if they cannot verify the basic elements of the transaction they must abstain from executing it, especially where there is suspicion of a connection with organised crime and terrorism activities.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes. Article 17 of Law 4557/2018 stipulates that credit institutions are prohibited from entering into or continuing a correspondent banking relationship with a shell bank and shall not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

3.9 What is the criteria for reporting suspicious activity?

Please see the answers to questions 3.4 and 3.5.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, through the General Electronic Commercial Registry (G.E.M.I) which keeps information on all legal forms of businesses in Greece.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, it is.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Ownership of legal entities in the form of bearer shares is permitted. However, for certain types of legal entities (such as banking institutions, telecommunications companies, etc.), the law provides that ownership is permitted solely in the form of registered shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Such requirements are established in decisions issued by the competent Ministries.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Yes, for instance, Law 4557/2018 has specific provisions regulating the operations of casinos.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Please refer to sections 2 and 3 above.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Following Law 4557/2018, which transposed the Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Greece's anti-money laundering efforts and tactics are in line with most European and international standards.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

In the 2007 Mutual Evaluation Report by the FATF, Greece was rated partially compliant or non-compliant for some Core and Key Recommendations. As a result, Greece was placed in the regular follow-up process. In February 2010, the FATF published the Interim Follow-Up Report. This report provided an update on progress made by Greece since 2007. In October 2011, the FATF recognised that Greece had made significant progress in addressing the deficiencies identified in the 2007 Mutual Evaluation Report and highlighted that Greece took sufficient action in remedying the identified deficiencies and that all the Core and all the Key Recommendations are at a level essentially equivalent to compliant (C) or largely compliant (LC). Currently, Greece is undergoing a new evaluation by the FAFT. Their findings are expected to be released in 2019.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Anti-money laundering legislation can be found at the Hellenic FIU's website at: http://www.hellenic-fiu.gr/.

Ilias Anagnostopoulos
Anagnostopoulos
6, Patriarchou Ioakeim
106 74, Athens
Greece

Tel: +30 210 729 2010
Email: ianagnostopoulos@iag.gr
URL: www.iag.gr

Ilias Anagnostopoulos, born in Piraeus, Greece, January 1956, was admitted to the Bar in 1981 (Athens). He received his education at the National University of Athens, School of Law (1978) and the Goethe University of Frankfurt am Main, Germany (*Dr. juris*, 1983). He was awarded the Tsirimokos Prize by the Hellenic Criminal Bar Association (1987).

Ilias has appeared as lead counsel in most significant criminal law cases in Greece during the past 25 years and has extensive experience in all types of business crime, financial fraud, insider dealing and market abuse, tax and customs fraud, medical malpractice, product criminal liability, environmental liability, art crimes, money laundering, corruption practices, anti-competitive practices and cartel offences, corporate criminal liability and compliance, anti-terrorism, European criminal law, extradition and mutual assistance.

In the *International Who's Who Legal of Business Crime Defence 2018*, Ilias ranks among the most highly regarded individuals ("Thought Leaders") worldwide and is described as "absolutely the go-to guy in Greece regarding corporate crime matters". Ilias chairs the Hellenic Criminal Bar Association (July 2013–) and is a Professor of criminal law and criminal procedure at the School of Law, National University of Athens.

He has published extensively in Greek, English and German on matters of Hellenic, European and international criminal law, business and financial crimes, reform of criminal procedure and human rights.

Alexandros Tsagkalidis
Anagnostopoulos
6, Patriarchou Ioakeim
106 74, Athens
Greece

Tel: +30 210 729 2010
Email: atsagkalidis@iag.gr
URL: www.iag.gr

Alexandros Tsagkalidis was born in Rhodes, Greece, in 1984 and was called to the Bar in 2009.

He received his education at the School of Law, National University of Athens (2007, LL.M. in Criminal Law, 2011). He is a member of the Legal Experts Advisory Panel of Fair Trials International and the Hellenic Criminal Bar Association. His practice focuses on money laundering and asset recovery, business crime, corruption practices, fraud, bribery, extradition and mutual assistance. Alexandros has published in Greek and English on matters of Asset Recovery, Investigation Procedures, Business Crimes and Defence Rights in the EU. He is fluent in Greek, English and French.

ANAGNOSTOPOULOS

Established in 1986, Anagnostopoulos is a leading practice combining high-value litigation services in all aspects of business crime with sophisticated advice in relation to criminal and regulatory risk management to corporations and individuals around the world. The firm offers a comprehensive range of services and enjoys an excellent reputation in a broad spectrum of specialist areas. It acts for some of the leading multinational and domestic corporations in the energy, raw materials, defence, aviation, shipping, automotive, construction, food, healthcare, pharmaceuticals, tobacco, financial services, travel and leisure, telecommunications and media and entertainment sectors. It is also entrusted with sensitive mandates by sovereign entities and public and governmental organisations.

Anagnostopoulos ranks among the country's premier providers of high-value litigation services and offers superior advice in managing criminal risks in complex matters with cross-jurisdictional aspects. The firm is noted for its expertise in cases involving corporate fraud, corruption, insider dealing, regulatory offences, money laundering, tax offences, anti-competitive practices, asset tracing and recovery. It has an impeccable record in offering discreet advice to corporate entities and high-net-worth individuals on a wide range of issues through multiple jurisdictions.

Chapter 14

India


Alina Arora


Bharat Chugh

L&L Partners Law Offices

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Prevention of Money Laundering Act, 2002 ("**PMLA**"), together with the rules issued thereunder and the rules and regulations prescribed by regulators such as the Reserve Bank of India ("**RBI**"), the Securities and Exchange Board of India ("**SEBI**") and Insurance Regulatory and Development Authority of India ("**IRDAI**"), sets out the broad framework for prosecution of money laundering in India with the Directorate of Enforcement ("**ED**") being empowered by the Federal Government to investigate and prosecute money laundering.

PMLA criminalises money laundering and allows for provisional attachment of 'proceeds of crime', which are likely to be concealed, transferred or dealt with in a manner that may obstruct proceedings. PMLA also seeks to prevent money laundering by mandating record-keeping and reporting obligations imposed on banks, financial institutions and intermediaries. The key rules and regulations pertaining to prevention and prosecution of money laundering are:

- the Prevention of Money Laundering (Maintenance of Records) Rules 2005, issued under the PML Act ("**PML Rules**");
- guidelines on Anti-Money Laundering (AML) Standards and Combating Financing Of Terrorism (CFT)/Obligations Of Securities Market Intermediaries Under Prevention Of Money-Laundering Act, 2002 And Rules Framed Thereunder ("**SEBI AML/CFT Guidelines**"); and
- the Master Direction – Know Your Customer ("**KYC**") Direction 2016 ("**RBI Directions**").

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

For the Government to bring a successful prosecution under the PMLA, it must establish that the accused directly or indirectly attempted to indulge or knowingly assisted or knowingly was a party or was involved in any process or activity connected with the 'proceeds of crime' including its concealment, possession, acquisition or use, and projecting or claiming it as untainted property.

PMLA defines proceeds of crimes as any property arising out of the commission of scheduled offences (predicate offences), with Schedule 1 of PMLA listing out the said offences.

Deconstructing the definition of 'proceeds of crime' reveals any property derived or obtained directly or indirectly by any person:

- as a result of criminal activity;
- relating to a 'scheduled offence'; or
- the value of any such property.

Scheduled offences range from those relating to corporate fraud, terrorism, illegal trade of arms, wildlife, narcotics to bribery of public officials. A wilful attempt to evade tax under section 51 of the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act 2015 is a scheduled offence.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

PMLA confers extra-territorial jurisdiction to the government to prosecute the offence of money laundering for "offences of cross-border implications" which arise when any proceeds of crime arising out of a scheduled offence committed in India have been remitted or attempted to be remitted outside India, or when conduct amounting to a scheduled offence has been committed outside India and any proceeds of crime therein may have been remitted to India. PMLA allows for attachment and confiscation of equivalent assets in India or overseas whenever the asset constituting the proceeds of crime is located abroad and cannot be forfeited.

PMLA empowers the Federal Government to enter into reciprocal arrangements with the government of any country outside India for enforcing the provisions of PMLA, and for the exchange of information for the prevention of any offence under PMLA or under the corresponding law in force in that country or for investigation under PMLA. As of today, the Indian government has executed Mutual Legal Assistance Treaties with 39 countries.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

While the ED is the nodal agency for investigation and prosecution of money laundering, however, given that commission of a scheduled offence is a prerequisite for initiation of proceedings for the offence of money laundering, the investigation of money laundering and the investigation of scheduled offences are tied together. The scheduled offence itself may be (and usually is) investigated by police or other investigating agencies. Thus, there

arises the need for cooperation and coordination between various investigating agencies. Hence, officers of various government entities are required to assist the authorities under the PMLA, including officers of the Customs and Central Excise Departments, RBI, SEBI, the Police, and the Income Tax Department.

1.5 Is there corporate criminal liability or only liability for natural persons?

The term 'person' under the PMLA has been defined to include individuals, companies, firms, associations of persons (whether incorporated or not), artificial juridical persons and agencies, offices and branches owned or controlled by any of the aforesaid.

It is pertinent to note that Section 70 of the PMLA contains an express provision for imposition of liability upon a body corporate as well as every person in charge of and responsible to, the body corporate for the conduct of its business at the time of the commission of the relevant offence. However, such a person may not be held liable, if, he is able to prove that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence. Further, in the event of any violation of the PMLA by a body corporate, where it is established that the offence has been committed with the consent or connivance of, or that the commission of the offence is attributable to any neglect on the part of any director, manager, secretary, or other officer of the company, such officer(s) may be liable to be proceeded against and punished accordingly.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Section 4 of the PMLA provides for rigorous imprisonment for a term between three to seven years, along with a fine for money laundering relating to all scheduled offences apart from offences pertaining to narcotics, wherein, the maximum term of imprisonment may extend to 10 years.

1.7 What is the statute of limitations for money laundering crimes?

PMLA does not specifically provide for a limitation period in relation to the offence of money laundering. Further, as per the law of limitations for criminal offences under Section 468 of the Criminal Procedure Code, 1973 ("CrPC"), there is no limitation period for offences punishable with imprisonment of more than three years, hence, for offences punishable under the PMLA, there is no limitation period.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

The PMLA is a federal legislation and is enforced by the federal government. Having said that, it may be noted that the PMLA has not repealed the Criminal Law Amendment Ordinance, 1944.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The PMLA provides that if the special court constituted under the PMLA concludes that the offence of money-laundering is made out, it shall order that such property involved in the money-laundering or which has been used for the commission of the offence of money-laundering shall stand confiscated to the federal government.

Further, the ED may provisionally, for a period of 180 days, attach properties of persons who, the ED has 'reason to believe' are in possession of the proceeds of crime and such proceeds are likely to be concealed, transferred or dealt with in any manner that may result in frustrating any proceedings. The same may later be confirmed by an 'Adjudicating Authority' appointed by the federal government. While attachment allows continued enjoyment to persons interested in the property, confiscation involves a government officer taking possession of the property. Further, in *B Rama Raju v Union of India*, the Andhra Pradesh High Court had held that for the purposes of attachment and confiscation, neither *mens rea* nor the knowledge of the criminal lineage of the property is required to be established. Hence, the authorities may attach/confiscate proceeds of crime in possession of persons who have not been charged with the predicate offence or the offence of money laundering.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Since jurisprudence relating to money laundering is at a nascent stage, it is only recently that trials have concluded, and convictions have been made in money-laundering cases. Having said that, there do not appear to be reported convictions of banks or regulated financial institutions.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Though the CrPC provides for the 'compounding' of certain offences with consent of parties involved or with consent of the court, the offence of money laundering under the PMLA cannot be compounded.

However, under the CrPC, the accused may apply for plea bargaining, for PMLA offences punishable with up to seven years of imprisonment. Plea bargaining implies that, upon mutual agreement between the victim, the accused and the prosecution, the accused pleads guilty and the Court thereafter may impose a lenient sentence. Plea bargaining is impermissible for the scheduled offence relating to narcotics, since the same is punishable with 10 years' imprisonment. Also, plea bargaining is unavailable for socio-economic offences and it is quite possible that the government may, in the future, notify the offence of money-laundering as a socio-economic offence owing to its very nature, rendering plea bargaining impermissible, and address this obvious lacuna.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Banks, financial institutions and intermediaries, and persons carrying out any designated business or profession, are classified as

reporting entities ("**REs**") under the PMLA and their obligations are primarily enshrined in Chapter IV of the PMLA. REs are, *inter alia*, required to comply with the following obligations:

(a) maintain a record of all transactions, in such manner as to enable it to reconstruct individual transactions for a period of five years from the date of the transaction between the client and the RE;

(b) furnish information to the Financial Intelligence Unit – India ("**FIU-IND**)", with respect to, *inter alia*, suspicious transactions, counterfeit currency transactions and all cash transactions in excess of a certain value including a series of interconnected transactions that may cumulatively amount to a prescribed value, to the FIU-IND within such time as may be prescribed, regardless of whether such transaction was attempted or executed;

(c) verify the identity of its clients and the beneficial owner in accordance with the customer due diligence ("**CDD**") requirements under Rule 9 of the PML Rules; and

(d) maintain a record of documents reflecting the identity of its clients and beneficial owners as well as correspondence and account details pertaining to the client.

The PML Rules prescribe exhaustive requirements for REs to establish and verify the identity of any client at the time of operating an account or executing a transaction, including prescribing the documents that the REs should seek from a client and maintain on record. The PML Rules also stipulate that the procedures and manner of maintenance of records may be prescribed by relevant regulators such as the RBI, SEBI and IRDAI, pursuant to which regulators have promulgated various directions and guidelines such as the SEBI AML/CFT Guidelines and the RBI Directions.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

There are no such requirements.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

No, they are not.

2.4 Are there requirements only at national level?

Yes. Rules and regulations are laid down by the authorities at the national level only (authorities such as those mentioned in the answer to question 2.1). There are no additional requirements at the state level. Further, requirements laid down are also monitored only at the national level by FIU-IND, which is an independent national level body reporting to the Economic Intelligence Council ("**EIC**") which is headed by the Finance Minister of the Central Government.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The FIU-IND was set up by the government of India in November 2004 and the Director of the FIU-IND has been vested with exclusive powers under Section 13 of the PMLA to monitor REs apropos compliance with anti-money laundering stipulations. Further, regulators such as the RBI, SEBI and IRDAI monitor compliance of REs with their sector-specific anti-money laundering directions/guidelines.

If the FIU-IND passes an order against a RE for non-compliance with anti-money laundering obligations under Section 12 of PMLA, such orders are publicly available on its website. It may be noted that the FIU-IND may choose to redact information in such orders, if it deems it fit. Moreover, orders issued by regulators for non-compliance with their sector-specific money laundering directives and norms are also available on their respective websites.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The FIU-IND was established by the federal government as the nodal agency for receiving, processing, analysing and disseminating information relating to suspect financial transactions, and it reports to the Economic Intelligence Council, chaired by Finance Minister, India. The FIU-IND coordinates between national and international intelligence and enforcement agencies and is a member of the Egmont Group, a multi-national collective tasked with enhancing cooperation amongst FIUs.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no limitation period under the PMLA for FIU-IND to bring an enforcement action for non-compliance by REs.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Section 13 of the PMLA empowers the FIU-IND to impose fines ranging from 10,000 rupees to 100,000 rupees on the RE, Designated Director or its officers for their failure to discharge their obligations pertaining to maintenance of records, reporting to the FIU-IND and undertaking due diligence on their clients and identifying beneficial ownership of clients, in accordance with Chapter IV of the PMLA and relevant PML Rules.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Apart from imposing a monetary penalty, non-compliance with Chapter IV of the PMLA by the RE may result in Director, FIU-IND:

(a) issuing a written warning;

(b) directing such RE or Designated Director or any of its employees, to comply with specific instructions; or

(c) directing such RE or Designated Director or any of its employees, to send reports at such interval as may be prescribed on the measures taken by RE.

Furthermore, regulators such as the RBI are empowered to revoke licences of REs under their respective jurisdictions for non-compliance with the directives/guidelines issued by them including anti-money laundering obligations.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Yes, the FIU-IND may impose only administrative/civil penalties upon REs for non-compliance with Chapter IV of the PMLA by the RE.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The FIU-IND is the competent authority for assessing the compliance of REs and is also empowered to seek information from REs to facilitate such assessment. The Director of FIU-IND may impose penalties in accordance with Section 13 of the PMLA, if, it determines that the RE has not honoured its requests for information and/or not complied with the applicable monitoring requirements. The decision of the FIU-IND in this regard may be appealed to the Appellate Tribunal set up under the PMLA.

All orders by the FIU-IND and the Appellate Tribunal are available on their respective websites.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Banks, financial institutions and intermediaries, and persons carrying out any designated business or profession, are classified as reporting entities under the PMLA.

The REs are defined as follows under the PMLA:

A "Banking company" means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 applies and includes any bank or banking institution referred to in section 51 of that Act.

A "financial institution" means a financial institution as defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a non-banking financial company and the Department of Posts in the Government of India.

An "intermediary" means: (i) a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992; (ii) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 or any member of such association; (iii) intermediary registered by the Pension Fund Regulatory and Development Authority; or (iv) a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956.

A "person carrying on designated business or profession" would include: (i) a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casinos; (ii) a Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908, as may be notified by the Central Government; (iii) a real estate agent, as may be notified by the Central Government; (iv) a dealer in precious metals, precious stones and other high value goods, as may be notified by the Central Government; (v) a person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government; or (vi) a person carrying on such other activities as the Central Government may, by notification, so designate, from time to time.

Please refer to the answer to question 2.1 for understanding the obligations imposed upon REs.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

RBI's circular dated April 6, 2018 ("**Circular**") banned all entities regulated by RBI which include banks, financial institutions, non-banking financial institutions, payment system providers, etc. from dealing in, or facilitating any dealings in, cryptocurrencies. The Supreme Court of India has been approached to urge the executive wing to clarify the policy on legality of cryptocurrency in India, including for the stated concern that cryptocurrency use is in, or poses, violation of the PMLA. The constitutional validity of the Circular has also been challenged. However, it may be noted that non-compliance with the Circular has not been made a scheduled (predicate) offence under the PMLA.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Record-keeping, monitoring and reporting of transactions (please see the answer to question 3.4), customer identification and CDD (please see the answer to question 3.7) are integral elements of a compliance programme expected to be maintained by REs.

It must be noted that Rule 9(14) (ii) of PML Rules mandates REs to implement a CDD Programme to determine the true identity of its clients, incorporating requirements under Rule 9 of PML Rules and guidelines issued by the relevant regulator under Rule 9(14)(i) of the PML Rules to verify the client's identity taking into consideration the type of client, business relationship or nature and value of transactions.

SEBI AML/CFT Guidelines require REs to adopt written procedures, which shall, *inter alia*, include the following three specific parameters which are related to the overall "**Client Due Diligence Process**":

(a) Policy for acceptance of clients.

(b) Procedure for identifying the clients.

(c) Transaction monitoring and reporting especially Suspicious Transactions Reporting ("**STR**").

Similarly, the RBI Directions require REs to promulgate a KYC policy duly approved by the Board of Directors of REs, which shall include the following elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures ("**CIP**"); and

(d) Monitoring of Transactions.

Furthermore, pursuant to the PML Rules and guidelines/directions by regulators, REs must appoint a principal officer who shall be

responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required by PMLA, including rules thereunder and by relevant regulators ("**Principal Officer**"). The Principal Officer is expected to be of a sufficiently senior position and able to discharge its functions with independence and authority.

Also, REs are required to designate a director on the Board of the Company or an equivalent position for other corporate structures to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and rules thereunder ("**Designated Director**"). It may be noted that the Principal Officer cannot be nominated as the 'Designated Director'.

Further, as part of such compliance requirements, REs and their directors, officers and employees (permanent and temporary) are prohibited from informing the client of any reports of suspicious transactions or related information being provided to the FIU-IND.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Pursuant to Rule 3 of the PML Rules, every RE is required to maintain a record of all transactions, including:

1) cash transactions in excess of 1 million rupees or its equivalent in foreign currency;
2) all series of cash transactions that are integrally connected to each other and that have been valued below 1 million rupees or its equivalent in foreign currency, where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds 1 million rupees;
3) all transactions involving receipts by not-for-profit organisations in excess of 1 million rupees or its equivalent in foreign currency;
4) all cash transactions where forged or counterfeit currency has been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
5) all 'suspicious transactions', including attempted transactions, whether made in cash or not, made by way of:
   a) deposits and credits, withdrawals into or from any accounts by way of cheques, travellers' cheques or transfer from one account to another within the same RE and any other mode in whatsoever name it is referred to;
   b) credits or debits into or from any non-monetary accounts such as demat accounts or security accounts, in any currency, maintained with the RE;
   c) money transfers or remittances in favour of clients or non-clients from India or abroad and to third-party beneficiaries in India or abroad, including transactions on its own account in any currency by any mode of money transfer;
   d) loans and advances including credit or loan substitutes, investments and contingent liability by way of subscription to debt instruments such as commercial paper, certificates of deposit, preferential shares, debentures, securitised participation, interbank participation or any other investments in securities, purchase and negotiation of bills, cheques and other instruments, foreign exchange contracts, currency, interest rate and commodity and any other derivatives, letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates or any other instrument for settlement or credit support; and
   e) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection;
6) all cross-border wire transfers in excess of 500,000 rupees or its equivalent in foreign currency where either the origin or destination of fund is in India; or
7) all purchase and sale by any person of immovable property valued at 5 million rupees or more that is registered by the RE. (Collectively "**Recorded Transactions**".)

Furthermore, Rule 4 of the PML Rules mandates that records pertaining to a transaction must contain all the necessary information specified by a relevant regulator to permit reconstruction of individual transactions, including the following information:

1) the nature of the transaction;
2) the amount of the transaction and the currency in which it was denominated;
3) the date on which the transaction was conducted; and
4) the parties to the transaction.

The PML Rules stipulate that the procedures and manner of maintenance of records, including records of transactions and identity of clients, may be prescribed by relevant regulators such as the RBI, SEBI and IRDAI, pursuant to which regulators have promulgated various directions and guidelines such as the SEBI AML/CFT Guidelines and the RBI Directions.

The Principal Officer is under an obligation to furnish information relating to suspicious transactions to the FIU-IND no later than seven working days on being satisfied that the transaction is suspicious, and all other Recorded Transactions, apart from sale and purchase of immovable property, are required to be reported by the 15th day of the succeeding month with information pertaining to sale and purchase of immovable property being reported to the FIU-IND every quarter by the 15th day of the month succeeding the quarter. Furthermore, various regulators prescribe their own reporting requirements.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There is no explicit requirement for routine reporting of transactions apart from large cash/suspicious transactions being reported to FIU-IND. Please refer to the answer to question 3.4.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Please refer to the answer to question 3.4 for details pertaining to the same.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Rule 9 of the PML Rules, *inter alia*, require that at the time of commencement of an account-based relationship, a RE must identify its clients, verify their identity as well as identify and verify the beneficial owners of the client, if any and obtain information on the purpose and intended nature of the business relationship. It may be noted that the relevant regulator may, in certain situations, permit

the RE to complete the verification as soon as reasonably practicable following the establishment of the relationship. In all other cases, the RE must verify identity while carrying out:

i) transactions of an amount equal to or exceeding 50,000 rupees whether conducted as a single transaction or several transactions that appear to be connected; or

ii) any international money transfer operations.

Further, there is an obligation on REs to exercise ongoing due diligence with respect to the business relationship with every client and closely examine transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, source of funds.

Pursuant to Rule 9(14)(i) of the PML Rules, various regulators have promulgated guidelines/directions for undertaking enhanced CDD to verify the client's identity.

As an example, the SEBI AML/CFT Guidelines recognise that certain clients may be of a higher or lower risk category with entities being required to undertake a risk assessment of the client depending on the client's background and location, type of business relationship, nature, or volume of transaction, payment methods, etc. The risk categorisation of customers into low, medium and high risk determines the nature and extent of information and documents required as part of the CDD process.

The SEBI AML/CFT Guidelines provides an illustrative list of Clients of Special Category ("**CSC**") which includes high-net-worth clients, trust, charities, non-governmental organisations, closely held companies, politically exposed persons ("**PEP**"), companies offering foreign exchange offerings or clients from high-risk countries, such as countries with suspect money laundering controls, unusual banking secrecy, narcotics production, highly prevalent corruption or countries reputed to be offshore financial centres and tax havens, non face-to-face clients and clients with dubious reputation, etc. It may be noted that additional requirements have been promulgated for PEPs under the SEBI AML/CFT Guidelines.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

RBI Directions mandate that correspondent relationships shall not be entered with a shell bank and correspondent banks shall not permit their accounts to be used by shell banks.

3.9 What is the criteria for reporting suspicious activity?

The term '*transaction*' has been defined under the PML Rules to include deposits, withdrawal and exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other nonphysical means. Any such transactions which:

(a) give rise to a reasonable ground of suspicion that it may involve proceeds of a scheduled offence;

(b) appears to be made in circumstances of unusual or unjustified complexity;

(c) appears to have no economic rationale or *bona fide* purpose; or

(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism,

is to be reported as a suspicious transaction, as per the PML Rules.

Transactions undertaken by designated persons subject to United Nations' Sanctions must be reported by REs along with the suspicious transaction reports submitted to the FIU-IND in the prescribed format.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, the Ministry of Corporate Affairs maintains a publicly searchable corporate registry.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

RBI Directions mandate that all international wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account number. However, interbank transfers and settlements wherein both the originator and beneficiary are banks or financial institutions are exempt. Domestic wire transfers above 50,000 rupees and above shall be accompanied by originator information such as name, address and account number. It may also be noted that RBI Directions require the Beneficiary bank to report a transaction lacking complete originator information to FIU-IND as a suspicious transaction.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No, Indian company law does not permit the use of bearer shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the reporting requirements for all businesses, including financial institutions stem from Chapter IV of the PMLA.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No, but Rule 9(13) of PML Rules requires REs to carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels that is consistent with any national risk assessment conducted by a body appointed by the Federal Government. It may be noted that India initiated a national risk assessment exercise in January 2016 to identify sectors which are vulnerable to money laundering.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

The Fugitive Economic Offenders Act, 2018 ("**FEO Act**") provides for measures to deter FEOs from evading the process of law in India by staying outside the jurisdiction of Indian courts. An FEO is any individual against whom a warrant for arrest in relation to a Scheduled Offence, as provided for in the FEO Act ("**FEO-scheduled offence**") has been issued by any Court in India, who has left India so as to avoid criminal prosecution; or being abroad, refuses to return to India to face criminal prosecution. The offence of money-laundering under the PMLA is an FEO-scheduled offence. The proceeds of crime in relation to the FEO-scheduled offence of money-laundering may be attached or confiscated as per a separate regime provided under the FEO Act, which are in addition to the PMLA itself.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

India is compliant with the recommendations of FATF. Please refer to the answer to question 4.3.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Pursuant to India's application for membership with the FATF, India was evaluated by FATF along with the Asia Pacific Group ("**Mutual Evaluation**") in 2009–10 to assess India's compliance with the 40+9 recommendations of the FATF. Subsequent to the Mutual Evaluation, India was placed under a regular follow up process, and in FATF's 8th follow-up report dated June 2013, it was concluded that India had reached a satisfactory level of compliance with the recommendations and India was placed out of the regular follow-up process. India is slated to undergo another on-site mutual evaluation by the FATF in November–December 2020.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The framework of laws governing the anti-money laundering regime is available on the website of FIU-IND and regulations promulgated by regulators such as the RBI are available on their respective websites.

Note

The authors of this article are Ms. Alina Arora who is a Corporate Partner and Mr. Bharat Chugh who is a Disputes Partner Designate at L&L Partners [formerly Luthra & Luthra Law Offices], New Delhi, India. The views of the authors expressed in this article are personal and do not necessarily reflect the views of the Firm. Please note that this publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither the Firm nor any member of the Firm can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Alina Arora

L&L Partners Law Offices
1st and 9th Floors, Ashoka Estate
24 Barakhamba Road
New Delhi – 110 001
India

Tel: +91 98715 92008
Email: aarora@luthra.com
URL: www.luthra.com

Ms. Alina Arora is a Partner with L&L Partners Law Offices specialising in the areas of Anti-corruption advisory, White Collar Crimes, Mergers and Acquisitions (M&A), Joint Ventures, Corporate advisory, Regulatory and Procurement advisory, Insurance and Private Equity.

Alina has led complex multi-jurisdictional internal investigations involving bribery, money laundering, accounting irregularities and other such related issues. In this regard, she has been actively engaged in providing advice relating to Indian anti-corruption laws such as the Prevention of Corruption Act, the Foreign Contributions Regulation Act, the Indian Penal Code as well as the Indian law implications of foreign enactments such as the Foreign Corrupt Practices Act and the UK Bribery Act. Further, she has considerable experience in conducting compliance audits and has also overseen post-acquisition compliance integration and compliance-driven restructuring of business.

Alina has been consistently recommended by *Chambers Asia-Pacific* for White Collar Crimes since 2014, including for 2019 and was also nominated as a leading practitioner for White Collar Crimes by *Expert Guides* 2018.

Bharat Chugh

L&L Partners Law Offices
1st and 9th Floors, Ashoka Estate
24 Barakhamba Road
New Delhi – 110 001
India

Tel: +91 98105 53252
Email: bchugh@luthra.com
URL: www.luthra.com

Mr. Bharat Chugh graduated in law in 2011 and in 2013, at the age of 23, secured First Rank in the Delhi Judicial Service Examination and joined as a Judge. In 2016, at the age of 27, he resigned from the service and returned to the practice of law.

As a Partner Designate at L&L Partners, Bharat represents clients on a wide range of issues with a strong focus on White Collar Crime and International Arbitration. Bharat has also been appointed as *amicus curiae* by the Delhi High Court in numerous serious criminal cases.

Bharat was also featured in the book: 'On the Rise: Inspiring Stories of Young Legal Professionals in India' in 2017.

INBA recently awarded Bharat the Young Lawyer of the Year (Male) Award in 2018.

Bharat has also served on various committees, including the Delhi High Court Committee on Arbitration. He currently serves on the Young SIAC Committee.

L&L PARTNERS
Law Offices

L&L Partners (formerly Luthra & Luthra Law Offices) is a leading full-service law firm, with a team of over 300 counsels including 73 partners, with offices at New Delhi, Mumbai, Bengaluru and Hyderabad. As part of the White-Collar Crimes practice, the Firm regularly advises clients on legal issues under Indian anti-corruption laws including the Prevention of Money Laundering Act, 2002, the Prevention of Corruption Act, 1988, along with allied laws and regulatory frameworks. We possess significant expertise in advising clients on Indian implications of US FCPA, 1977 and UK Bribery Act, 2010. The Firm has advised several high-profile multinational clients across sectors, including banking, financial services, insurance, aerospace, defence, and alcohol, be it for, conducting internal investigations or white-collar defence.

Consistently ranked and globally recognised as leaders in the field, we adopt a forward-looking approach towards the practice of law, combining both conventional practice areas & emerging sectors, setting benchmarks and the highest technical standards within the legal fraternity.

Ireland

Darragh Murphy

McCann FitzGerald

Meghan Hooper

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Director of Public Prosecutions ("**DPP**") is responsible for the prosecution of crime in Ireland, including money laundering and terrorist financing.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The criminal offence of money laundering is set out in section 7 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended (the "**AML Act**"). According to that section, to establish the criminal offence of money laundering, the prosecution must prove that the defendant engaged in certain acts in relation to property that is the proceeds of criminal conduct while knowing or believing or being reckless as to whether the property is the proceeds of criminal conduct.

Consequently, the prosecution must prove that the defendant:

a) concealed or disguised the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;

b) converted, transferred, handled, acquired, possessed or used the property; or

c) removed the property from, or brought the property into, Ireland.

According to section 6 of the AML Act, the term "proceeds of criminal conduct" means any property that is directly or indirectly, entirely or partially, derived from or obtained through "criminal conduct". "Criminal conduct" means any conduct that constitutes an offence under Irish law, including tax evasion. It also means certain conduct that occurs outside of Ireland.

According to section 7(5) of the AML Act, a person will be reckless as to whether or not property is the proceeds of criminal conduct if the person disregards, in relation to property, a risk of such a nature and degree that, considering the circumstances in which the person carries out the acts set out above, the disregard of that risk involves culpability of a high degree.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Section 8 of the AML Act outlines certain circumstances where there is extraterritorial jurisdiction for the crime of money laundering. In particular, under section 8(1)(c) of the AML Act, an Irish citizen, a person who is an ordinary resident in Ireland, or a company established under Irish law or registered under the Companies Act 2014 will commit the offence of money laundering if that person or company engages in conduct in another jurisdiction in circumstances where the relevant conduct is an offence in the relevant jurisdiction and would be an offence under section 7 of the AML Act if the person engaged in that conduct in Ireland.

Money laundering of the proceeds of foreign offences is punishable as long as that conduct: a) is an offence in the place where it occurred, and would be an offence if it occurred in Ireland; or b) involves the bribery of a foreign public official under the Criminal Justice (Corruption Offences) Act 2018 (irrespective of whether it is considered to be bribery in the place where it occurred).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Garda Síochána (Gardaí), which is the Irish national police force, is responsible for investigating money laundering criminal offences. Within the Gardaí, the Garda National Economic Crime Bureau ("**GNECB**") is responsible for investigating serious and complex economic crimes as well as the investigation of financial crimes which are of major public concern. It also provides support and assistance to local and regional investigators, among other things. Ireland's Financial Intelligence Unit ("**FIU**") is embedded within the GNECB, which also houses two Money Laundering Investigation Units.

The DPP is responsible for prosecuting money laundering and terrorist financing offences. The Gardaí may decide to prosecute in less serious crimes, however, the prosecution is still taken in the name of the DPP and the DPP has the right to tell the Gardaí how to deal with the case.

1.5 Is there corporate criminal liability or only liability for natural persons?

Under Irish law, both natural persons and corporates can be held criminally liable. There is, however, some uncertainty about the test to be applied to determine how corporates can be held to account for criminal offences.

Section 111 of the AML Act provides for a form of derivative managerial responsibility which makes it possible to impose criminal liability on specified natural persons in circumstances where a body corporate commits a money laundering offence and it is proved that the offence was committed with the consent or connivance or is attributable to the wilful neglect of the relevant person. This section applies to:

(a) a director, manager, secretary or other officer of the body, or a person purporting to act in that capacity; and

(b) a member of the management committee or other controlling authority of the body, or a person purporting to act in that capacity.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalty applicable to individuals and legal entities convicted of money laundering under section 7 of the AML Act is up to 14 years' imprisonment and/or an unlimited fine.

1.7 What is the statute of limitations for money laundering crimes?

Under Irish law, there is no statute of limitations for offences that are prosecuted on indictment (i.e. trial by jury).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Enforcement is only at national level. Ireland does not have parallel state or provincial criminal offences.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Ireland has a strong legislative framework for asset confiscation on both a criminal and non-criminal basis. Confiscation of the proceeds of crime is governed by the Criminal Justice Act 1994 (as amended), which empowers the DPP to apply to court for a confiscation order where the defendant has been convicted of certain offences including money laundering and terrorist offences.

Under the Proceeds of Crime Act 1996–2016, the Criminal Assets Bureau ("**CAB**") can freeze and seize assets which it shows to the High Court are the proceeds of criminal conduct, on the balance of probabilities. CAB is a statutory, multi-agency body established under the Criminal Assets Bureau Act 1996 which consists of police officers, customs officers, tax officers and benefit agency personnel.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

While there have been a number of convictions for money laundering, information about the defendants in those cases is not easily accessible. We are not aware of situations where banks or other regulated financial institutions have been convicted of money laundering.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The DPP decides whether or not to prosecute a person for committing an offence and what the charge should be. For example, the DPP may decide not to prosecute an offence because of insufficient evidence, or because the prosecution is not in the public interest. The DPP cannot settle cases with an accused or engage in plea bargaining.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The AML Act imposes anti-money laundering requirements on certain "designated persons" including financial institutions. The Central Bank of Ireland (the "**Central Bank**") is responsible for monitoring compliance with the anti-money laundering requirements imposed on credit and financial institutions.

Each designated person must carry out and document a business risk assessment, to identify and assess the money laundering and terrorist financing ("**ML/TF**") risks involved in carrying on its business activities, taking into account the risk factors set out in Section 30A of the AML Act. It must also carry out a customer risk assessment in order to determine the type of customer due diligence to apply.

A designated person must also comply with customer due diligence requirements. Specifically, it must identify and verify the identity of its customers, their beneficial owners and persons purporting to act on behalf of a customer. Moreover, in the case of a business relationship, it must obtain information reasonably warranted by the risk of money laundering or terrorist financing on the purpose and intended nature of the business relationship, and monitor that relationship on an ongoing basis. A designated person must also examine the background and purpose of all complex or unusually large transactions and all unusual patters of transactions, which have no apparent economic or lawful purpose.

A designated person must report suspicious transactions to the Gardaí and Revenue.

The AML Act also requires each designated person to: put in place anti-money laundering policies and procedures; train staff on compliance with their anti-money laundering obligations; and keep records evidencing the designated person's AML compliance.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Generally, anti-money laundering requirements are set out in the AML Act; however, some self-regulatory organisations or professional associations have published guidance regarding these requirements.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, in some instances. The AML Act specifies the competent authorities responsible for monitoring specific categories of designated persons as well as empowering the Minister for Justice to prescribe a competent authority for a class of designated persons. Competent authorities include the Law Society of Ireland for solicitors and the designated accountancy bodies for auditors, external accountants or tax advisers.

2.4 Are there requirements only at national level?

Yes, the AML requirements apply at national level and there are no additional regional requirements.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The AML Act sets out the competent authorities that are responsible for monitoring compliance with the anti-money laundering requirements, including the Central Bank which is the competent authority for credit and financial institutions. While failing to comply with anti-money laundering requirements is an offence, the Central Bank also has the power to impose administrative sanctions for infringement of the anti-money laundering requirements.

The AML Act sets out what is required by way of compliance with anti-money laundering requirements and some competent authorities have supplemented these requirements with publicly available guidance. For example, the Central Bank publishes an Anti-Money Laundering Bulletin setting out its expectations regarding aspects of anti-money laundering. It has also published a number of sectoral reports setting out its observations and expectations in relation to anti-money laundering compliance, following on from on-site inspections conducted by the Central Bank.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, there is an FIU, which is responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements and which is embedded within the GNECB.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitations for offences that are prosecuted on indictment. Nevertheless, the Irish Constitution affords every accused the right to an expeditious trial. If there is inordinate or unconstitutional delay in the prosecution of a serious offence to the extent that there is a real risk of an unfair trial, a court may refuse to proceed with a prosecution.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Failure to comply with the anti-money laundering requirements is a criminal offence. For example, failure to identify and verify a customer can result in a fine and/or up to five years' imprisonment. Moreover, failure to comply with the anti-money laundering requirements by a regulated financial services provider ("**RFSP**") may also be subject to an administrative sanctions procedure. For example, under the Central Bank Act 1942, as amended (the "**1942 Act**"), the Central Bank has the power to impose fines of up to €10,000,000 or 10% of turnover on an RFSP and a fine of up to €1 million on a natural person involved in the failure to comply on the part of the RFSP.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Under the 1942 Act, the Central Bank can impose a wide range of administrative sanctions on an RFSP including a:

- caution or reprimand;
- direction to refund or withhold all or part of the money charged or paid, or to be charged or paid, for the provision of a financial service by a RFSP;
- in the case of a RFSP which is not authorised by the European Central Bank under the Single Supervisory Mechanism Regulations, suspension or revocation of the authorisation of that RFSP;
- in the case of a RFSP which is authorised by the European Central Bank under the Single Supervisory Mechanism Regulations, the submission of a proposal to the European Central Bank to suspend or revoke the authorisation of that RFSP;
- in the case of a natural person, a direction disqualifying the person from being concerned in the management of a RFSP for a prescribed period of time;
- direction to cease a contravention, if it is found the contravention is continuing; and
- direction to pay the Central Bank all or part of the costs incurred by the Central Bank in holding an inquiry and in investigating the matter to which the inquiry relates.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Violations of anti-money laundering obligations may be subject to criminal and administrative sanctions. However, provisions against double jeopardy may apply.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process of assessment and collection of sanctions and appeal of administration decisions depends on the relevant competent

authority. In the case of the Central Bank, the relevant process is set out in the 1942 Act. The Central Bank publishes resolutions of penalty actions, including settlements. We are not aware of instances where financial institutions have challenged AML-related penalty assessments in judicial proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The AML Act imposes anti-money laundering obligations on "designated persons" when acting in Ireland, in the course of business carried on in Ireland. The term "designated persons" is defined to include a "financial institution", which in turn is defined to include banks, investment firms, insurers, insurance intermediaries, and collective investment undertakings.

The term "financial institution" also covers undertakings carrying on specified types of activities, such as lending, financial leasing, payment services, guarantees and commitments, trading in certain types of instruments, participating in securities issues and providing related services, money broking, portfolio management, safekeeping and administration of securities, safe custody services and issuing electronic money.

Certain non-financial institutions are also subject to anti-money laundering requirements, including, for example, property service providers, casinos as well as to any persons trading in goods in respect of transactions involving payments in cash of a total of at least €10,000.

The obligations imposed on designated persons are set out above. In addition to those obligations, section 108A of the AML Act requires financial institutions and persons that carry on the business of a cheque cashing office that are not authorised or licenced by the Central Bank to register with the bank.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The anti-money laundering requirements do not specifically apply to the cryptocurrency industry. They do, however, apply to those entities involved in cryptocurrency to the extent that the relevant entity falls within the definition of a designated person for the purpose of the AML Act. Moreover, Ireland is in the process of transposing the EU's Fifth Money Laundering Directive 2018/843 ("**MLD5**") into Irish law, which extends AML requirements to cover certain virtual currency exchanges and custodian wallet providers.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

The Central Bank is not empowered to impose a compliance programme on a financial institution or designated business, however, having such a programme is typically a condition of authorisation. In addition, the Central Bank may apply additional supervisory measures to firms and sectors to further mitigate against the risk of the financial services industry being exploited for ML/TF purposes. For example, the Central Bank has appointed Relationship Managers to certain firms and sectors in order to ensure appropriate responses and timely interventions to matters that arise. In addition, the Central Bank may meet with key control functions within firms, e.g., CEO, CRO, Internal Audit, Independent Non-Executive Directors, as well as attending board meetings in order to determine that firms are aware of ML/TF risks and that appropriate measures are being taken to mitigate those risks.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There are no specific requirements applicable to large currency transactions or record-keeping in relation to such transactions.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There are no such cash transaction reporting requirements.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There are no such requirements.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Each Designated Person must identify its customer and any person purporting to act on its customers behalf and verify their respective identities on the basis of documents or information that it has reasonable grounds to believe is reliable. In addition, a Designated Person must identify any beneficial owner connected with the customer and take measures reasonably warranted by the risk of money laundering and/or terrorist financing to verify the beneficial owner's identity to the extent necessary to ensure that the designated person has reasonable grounds to believe that it knows who the customer's beneficial owners are. Where the beneficial owner is a legal person, the Designated Person must take the measures reasonably warranted to understand the ownership and control structure of the entity or arrangement concerned.

A Designated Person must obtain information reasonably warranted by the risk of money laundering or terrorist financing on the purpose and intended nature of a business relationship with a customer prior to establishing the relationship. It must also monitor any business relationship with a customer to the extent reasonably warranted by the risk of money laundering or terrorist financing. A Designated Person must examine the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

A Designated Person must apply enhanced customer due diligence to:

- a correspondent banking relationship with another credit institution located outside of the EU;

- a business relationship or transaction with a Politically Exposed Person (a "**PEP**");
- customers resident in high-risk third countries; and
- a situation where a high-risk customer or business scenario is identified and there is a suspicion of money laundering or terrorist financing.

A Designated Person must obtain senior management approval before entering into or continuing a business relationship with a PEP or before entering into a correspondent banking relationship.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Section 59(1) of the AML Act prohibits credit institutions and financial institutions from entering into a correspondent relationship with a shell bank.

3.9 What is the criteria for reporting suspicious activity?

A Designated Person must report suspicious activity where it knows, suspects or has reasonable grounds to suspect, on the basis of information obtained in the course of carrying on business as a designated person, that another person has been or is engaged in the offence of money laundering or terrorist financing.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The EU (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019 (the "2019 Regulations") require an in-scope corporate entity to file its beneficial ownership information with the Register of Beneficial Ownership of Companies and Industrial Provident Societies, from 23 June 2019.

Corporate entities were previously required to keep a beneficial ownership register containing adequate, accurate and current information on their beneficial owners under the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016. These regulations have now been replaced with the 2019 Regulations, with effect from 22 March 2019.

A similar obligation to keep a beneficial ownership register is imposed on a trustee of an express trust under the European Union (Anti-Money Laundering Beneficial Ownership of Trusts) Regulations 2019. In order for this obligation to apply, either the trustee must be resident in Ireland or the trust must be otherwise administered in Ireland.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Under Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (the Wire Transfer Regulation) the payer's payment service provider ("**PSP**") must ensure that transfers of funds are accompanied by: the payer's name; the payer's payment account number; and the payer's address, official personal document number, customer identification number or date and place of birth. The payer's PSP must also ensure that transfers of funds are accompanied by the payee's name and payment account number.

The Regulation applies to transfers of funds, in any currency that are sent or received by a PSP or an intermediary PSP established in the EU. The term "funds" is defined in Article 3(8) of the Wire Transfer Regulation to mean banknotes and coins, scriptural money and electronic money.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The Companies Act 2014 prohibits bearer shares in respect of private companies.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Certain non-financial institutions are subject to anti-money laundering requirements, including, for example, property service providers, casinos as well as to any persons trading in goods in respect of transactions involving payments in cash of a total of at least €10,000.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

There are no specific anti-money laundering requirements imposed on such business and sectors.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

As outlined above, the Irish government is currently transposing MLD5 into Irish law.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

According to the FATF's most recent evaluation, Ireland has a sound and substantially effective regime to tackle money laundering and terrorist financing, but could do more to obtain money laundering and terrorist financing convictions and demonstrate its effectiveness in confiscating proceeds of crime.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Ireland's anti-money laundering regime was last evaluated by the FATF in September 2017.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The Electronic Irish Statute Book includes the Acts of the Oireachtas (Parliament) and statutory instruments. Material published by the Central Bank may be obtained on its website. The materials are publicly available in English.

Darragh Murphy
McCann FitzGerald
Riverside One, Sir John Rogerson's Quay
Grand Canal Dock
Dublin 2, D02 X576
Ireland

Tel: +353 1 607 1433
Email: Darragh.Murphy@mccanfitzgerald.com
URL: www.mccannfitzgerald.com

Darragh specialises in advising on regulatory and commercial matters relevant to financial services businesses, including insurance undertakings, investment management operations, fund promoters, banking entities and payment service providers.

Darragh's practice covers all aspects of carrying on regulated financial services activities in Ireland whether in relation to the authorisation of entities in this sector, their ongoing business requirements (customer, counterparty and/or regulator facing) and/or problem resolution. He advises extensively on anti-money laundering compliance and his clients include both regulated and unregulated entities.

Megan Hooper
McCann FitzGerald
Riverside One, Sir John Rogerson's Quay
Grand Canal Dock
Dublin 2, D02 X576
Ireland

Tel: +353 1 611 9158
Email: Megan.Hooper@mccannfitzgerald.com
URL: www.mccannfitzgerald.com

Megan is an experienced commercial litigation solicitor, advising companies and financial institutions on corporate disputes, internal investigations, as well as on regulatory and other statutory investigations and inquiries. She deals with dispute resolution through Commercial Court litigation and mediation. Since February 2009, she has acted as lead adviser to two financial institutions in relation to regulatory and criminal investigations arising from legacy issues.

She has expert knowledge about the procedures of the Garda National Economic Crime Bureau, the Director of Public Prosecutions and regulatory bodies such as the Chartered Accountants Regulatory Board, the Central Bank of Ireland and the Office of the Director of Corporate Enforcement. She has experience advising on suspicious transaction reports and responding to orders and statutory requests under the Central Bank Administrative Sanctions Procedure as well as other legislation. Megan also has experience dealing with data protection and customer confidentiality issues.

McCann FitzGerald

With over 600 people, including 400 lawyers and professional staff, McCann FitzGerald is one of Ireland's premier law firms. Our principal office is located in Dublin and we have overseas offices in London, New York and Brussels.

McCann FitzGerald offers a full range of services to corporate, financial service and industrial companies. Our Finance Group offers market-leading expertise across the full spectrum of financial products, including aviation and asset financing, corporate and investment lending, capital markets, derivatives, fintech, insurance, investment management, projects and infrastructure finance, real estate finance, restructuring and insolvency, securitisations, and structured finance.

We also advise banks and financial service providers on anti-money laundering and other regulatory compliance issues, enforcement of guarantees and security, dispute negotiations, employment disputes, breach of confidence & defamation claims and discovery orders and information requests.

McCann FitzGerald's clients include international organisations, major domestic entities and emerging Irish companies. We also work with many clients in the state and semi-state sectors.

Isle of Man

Sinead O'Connor

Kirsten Middleton

DQ Advocates Limited

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The legal authority to prosecute money laundering at national level is the Proceeds of Crime Act 2008 ("POCA"). It is very similar in content to the UK Proceeds of Crime Act and received Royal Assent on 21 October 2008.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

POCA states that money laundering is an act which: (a) constitutes an offence under section 139, 140 or 141; (b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (c); (c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a); or (d) would constitute an offence under paragraphs (a), (b) or (c) if done on the Island. A section 139 offence is the offence of concealing, disguising, converting, transferring or removing criminal property from the Island. A section 140 offence is the offence of becoming concerned in an arrangement which the person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. A section 141 offence is the offence of acquiring, using or having possession of criminal property. Property is criminal property if: (i) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or in part and whether directly or indirectly); and (ii) the alleged offender knows or suspects that it constitutes or represents such a benefit. Criminal conduct is conduct which: (a) constitutes an offence in the Island; or (b) would constitute an offence in the Island if it occurred there.

POCA does not specify which predicate offences are included but as the predecessor legislation extended to all crimes, POCA would apply to any crime which generated money to be laundered. This is inclusive of tax evasion.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

There are provisions within POCA for enforcement of a confiscation order where the property in question is outside of the Island or there may be evidence of criminal conduct outside the Island. There are also provisions for co-operation with external authorities who make requests for assistance. As set out in question 1.2, if the criminal conduct occurred outside of the Island, it is punishable if the criminal conduct would constitute an offence in the Island if it occurred there.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

It is the responsibility of the Economic Crime Unit to investigate money laundering offences, which then in turn passes the information to the Attorney Generals Chambers for prosecution (as applicable).

1.5 Is there corporate criminal liability or only liability for natural persons?

Section 221 of POCA states that where an offence under the Act is committed by a body corporate and it is proved that the offence: (a) was committed with the consent and connivance of an officer of the body; or (b) was attributable to neglect on the part of an officer of the body, the officer, as well as the body, shall be guilty of the offence.

There is also corporate criminal liability under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 (as amended 2018) (the "Code"). The Code is secondary legislation made under POCA which requires relevant businesses to have anti-money laundering and countering the financing of terrorism procedures and controls in place.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

A person guilty of an offence as set out in question 1.2 above is liable on summary conviction to custody for a term not exceeding 12 months, or to a fine not exceeding £5,000, or both; or on conviction on information, to custody for a term not exceeding 14 years, or to a fine or both.

1.7 What is the statute of limitations for money laundering crimes?

There is no prescribed statute of limitations in respect of criminal conduct which can give rise to criminal property.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Enforcement is only at national level. There are no states or provinces in the Isle of Man.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

POCA provides for recovery orders, property freezing orders, interim receiving orders, recovery of cash, confiscation orders and restraint orders.

Proceedings for a recovery order may be taken by the Attorney General in the High Court against any person who the Attorney General thinks holds recoverable property. There are extensive provisions in POCA as to what is and is not recoverable property but it is, in essence, property obtained through unlawful conduct.

Where the Attorney General may take proceedings for a recovery order in the High Court, the Attorney General may apply to the court for a property freezing order. He may also apply for an interim receiving order.

There are provisions for the seizure and detention of cash if a customs officer or police constable suspects that the cash is recoverable property or is intended for use by any person in unlawful conduct.

The Court of General Gaol Delivery can make a confiscation order if it (a) decides that the defendant has a criminal lifestyle and has benefited from his or her general criminal conduct, or (b) it decides that the defendant does not have a criminal lifestyle and has benefited from his or her particular criminal conduct. POCA does contain provisions as to what constitutes a criminal lifestyle and what constitutes conduct and benefit.

The Court of General Gaol Delivery can make a restraint order, subject to a condition for such an order being in place, prohibiting any specified person from dealing with any realisable property held by that person. Realisable property is itself defined in POCA.

Conduct occurring in the Island is unlawful conduct if it is unlawful under the criminal law. Conduct which occurs outside the Island and which would be unlawful under the criminal law of the particular country and unlawful under the criminal law of the Island is also unlawful conduct. The court must decide on a balance of probabilities whether it is proved (a) that any matters alleged to constitute unlawful conduct have occurred, or (b) that any person intended to use any cash in unlawful conduct.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

The most recent significant conviction of money laundering in this context was in 2009 when directors of a trust and corporate service provider were convicted of money laundering and false accounting. The Council of Europe body MONEYVAL, of which the Isle of Man is a member, said in its 2017 report that the Island had a modest rate of convictions and this was identified as a weakness in the Island's AML/CFT regime. It is anticipated, therefore, that authorities will seek opportunities to bring prosecutions where possible. In 2018, proceedings were started against two former employees of a trust and corporate service provider for failure to disclose offences and the offence of becoming concerned in an arrangement. It is understood that these relate to possible offences under the counter financing of terrorism legislation. These proceedings have not yet been concluded.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

In some circumstances, criminal actions can be resolved outside of the judicial process by way of settlement agreements; similar to the Deferred Prosecution Agreements introduced in the UK. Whilst the agreements are typically private agreements, any hearing of the Court to sanction/approve the agreement may be open to the public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Aside from the primary legislation (POCA, the Anti-Terrorism and Crime Act 2003 and the Terrorism and Other Crime (Financial Restrictions) Act 2014), the Code, as referred to in question 1.5, also imposes AML requirements on financial institutions and other businesses. In addition, the Isle of Man Financial Services Authority (the "FSA"), which is the principal supervisor of financial institutions and designated non-financial businesses and professions ("DNFBPs"), has issued a comprehensive AML/CFT Handbook (the "Handbook") which sets out how the provisions of the Code should be met.

The Gambling Supervision Commission (the "GSC") is the principal supervisor of the e-gaming and terrestrial gaming sector. Whilst the primary legislation applies equally to the gambling sector, there is a gaming specific version of the Code and also a separate AML/CFT Handbook issued by the GSC.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

It is likely that the professional associations in the accountancy sector have anti-money laundering requirements which are imposed on member firms in the Isle of Man. As these requirements are UK based and do not take account of Isle of Man AML/CFT legislation and regulation, compliance with the Isle of Man standards will normally ensure compliance with any UK-based standards. Island members of such professional associations would normally look to the FSA's Handbook for the standards of conduct expected.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The FSA is the principal supervisor of all financial institutions and DNFBPs. Although supervision through on-site visits of some of the DNFBPs has been delegated to the self-regulatory organisations or professional associations with which the FSA has a Memorandum of Understanding, the FSA remains responsible for enforcement.

2.4 Are there requirements only at national level?

Due to the size of the Isle of Man, there are only requirements at national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The FSA is responsible for examination of compliance and enforcement of anti-money laundering requirements for financial institutions and DNFBPs. The GSC is responsible for examination of compliance and enforcement of anti-money laundering requirements for gaming operators. The FSA's supervisory approach is normally publicly available. That of the GSC does not appear to be publicly available.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

There is a Financial Intelligence Unit (the "FIU") which is under the direction of a Board comprised of the Attorney General, the Chief Constable and the Collector of Customs & Excise. Financial institutions, DNFBPs and gaming operators are all required to report to the FIU via the online portal THEMIS.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no prescribed limitation upon which a competent authority must bring enforcement actions under legislation.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

A breach of the Code and its gaming equivalent carries a penalty of: (a) on summary conviction to custody for a term not exceeding 12 months or to a fine not exceeding £5,000 or both; or (b) on conviction on information, to custody not exceeding two years or to a fine or both. The FSA has powers under the Financial Services (Civil Penalties) Regulations 2015 to levy a civil penalty. Where there is a Level One issue (risk of loss), the FSA can fine the licence holder up to 5% of relevant income. Where there is a Level Two issue (actual loss), the FSA can fine the licence holder up to 8% of relevant income. The FSA has used its civil powers in respect of a licence holder who was also convicted of a breach of the Code. The penalty levied by the courts for breach of the Code was in the region of £45,000. The civil penalty levied by the FSA was in the region of £90,000. The Financial Services Act 2008 gives the FSA a range of additional powers which could be used in the event of AML/CFT compliance failures including not fit and proper directions, prohibitions and ultimately the revocation of a licence. A consultation has been launched in February 2019 for the introduction of the Anti-Money Laundering and Countering the Financing of Terrorism (Civil Penalties) Regulations 2019 (the "proposed Regulations"). These proposed Regulations would enable the FSA to impose a penalty of up to 8% of the relevant person's income where there is a material breach of the Code and £50 per contravention where breaches are less material.

The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018 provides the GSC with similar powers to the FSA including the ability to levy civil penalties. The proposed Regulations do not extend to the GSC.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The FSA and the GSC have a range of sanctions available to them including restriction of activities, licence conditions, directions, public statements, injunctions, warning notices, appointment of skilled persons, prohibitions and revocation of the licence.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

A breach of the Code would be criminal as would any offence under the primary legislation.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

There is an appeal process set out in the Financial Services Act 2008 in relation to decisions made by the FSA. There is a Financial Services Tribunal which would hear any appeal. Some measures taken by the FSA, for example, a warning notice, might not be made public but an appeal to the Tribunal would usually be in the public domain. Similarly, there is a Gambling Appeals Tribunal which would hear any appeal under the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Schedule Four to POCA sets out which types of business qualify as a 'business in the regulated sector' for the purposes of POCA and the Code. There is a wide range of businesses captured which includes the traditional financial services sector (banking, insurance, funds), as well as the gaming sector (online and terrestrial), estate agents, lawyers (when they undertake certain types of activities), accountants, corporate and trust service providers, pension providers, money transmission agents, tax advisers, charities, payroll agents and those businesses involved with virtual currency.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

As per the answer to question 3.1, businesses involved with virtual currency are deemed to be a business in the regulated sector and have to comply with the Code. The wording of Section Four of

POCA is widely drawn and encompasses the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies including crypto currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity. Any business which falls into this definition must register with the FSA as a DNFBP and is subject to the FSA's supervision for compliance with the Code and the FSA's AML/CFT Handbook.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Any business which qualifies as a 'business in the regulated sector' (see question 3.1 above) is required to comply with the Code. Paragraph 29 of the Code requires such a business to maintain appropriate procedures for monitoring and testing compliance with the AML/CFT requirements having regard to ensuring that: (a) the business has robust and documented arrangements for managing the risks identified by the business risk assessment; (b) the operational performance of those arrangements is suitably monitored; and (c) prompt action is taken to remedy any deficiencies in arrangements.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

In accordance with the Customs & Excise Management Act 1986, Customs & Excise issued Notice 9011 (the "Notice") in November 2008. The Notice states that if cash in excess of €10,000 is sent to or taken from, or is brought into or received in the Island, then the person carrying, sending or receiving it must make a declaration to Customs & Excise. This applies to cash going to or coming from anywhere outside the Island and regardless of whether the cash is being carried by someone or is sent in the mail, by courier service or is contained in freight, a vehicle or a vessel. Cash includes any banknotes or coins in any currency (including counterfeit), postal orders and cheques of any kind (including travellers' cheques) but excluding cheques drawn on a British or Irish bank. It also includes stored value cards, and other documents, devices, coins or tokens with a monetary value.

Paragraph 9 of the Code requires a business in the regulated sector to perform ongoing and effective monitoring of any business relationship which includes appropriate scrutiny of transactions paying particular attention to suspicious and unusual activity. Unusual activity is defined in the Code to include large transactions. There is no definition or threshold for 'large' so each business would have to consider that in the context of their customer relationship.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There is a requirement to report any suspicious transaction to the FIU.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Aside from the requirements of Notice 9011 set out in question 3.4, Isle of Man financial institutions also have to comply with the US Foreign Account Tax Compliance Act and the Common Reporting Standard. These require automatic exchange of information on accounts and balances held by residents of various other jurisdictions. Reporting by Isle of Man financial institutions is to the Isle of Man Income Tax Division which then exchanges the information with other tax authorities around the world.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

The customer due diligence requirements are set out in the Code. These broadly require: (a) the identification of the customer; (b) the verification of the identity of the customer using reliable, independent source documents; (c) the verification of the legal status of the customer using relevant information obtained from a reliable independent source; (d) the obtaining of information on the nature and intended purposes of the business relationship; and (e) the taking of reasonable measures to establish the source of funds. The FSA's Handbook provides further guidance on each of these areas.

Enhanced customer due diligence ("EDD") must be obtained (a) where a customer poses a higher risk of ML/TF as assessed by the customer risk assessment, or (b) in the event of any unusual activity. EDD is only required for a politically exposed person if there is a higher risk of ML/TF.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Paragraph 38 of the Code states that a business subject to the Code must not enter into or continue a business relationship or occasional transaction with a shell bank. Such a business must also take adequate measures to ensure that it does not enter into or continue a business relationship or occasional transaction with a respondent institution that permits its accounts to be used by a shell bank.

3.9 What is the criteria for reporting suspicious activity?

Section 142 of POCA creates the failure to disclose an offence on the basis of four conditions being present. These are, in summary: (1) there is knowledge or suspicion or reasonable grounds for knowing or suspecting that another is engaged in money laundering; (2) that knowledge or suspicion or reasonable grounds came from business in the regulated sector; (3) the identity of the person mentioned in (1) or the whereabouts of the laundered property is known or there is information that may assist in that regard; and (4) a disclosure is not made to the FIU.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Under the Beneficial Ownership Act 2017, there is a central register of beneficial owners of Isle of Man companies. This is, however, a private register and is only available to certain authorities via formal requests. It is not accessible by Isle of Man financial institutions other than to enter their own information.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

The Island has implemented the EU Directive in relation to wire transfers through an Order and Regulations. In accordance with the Directive, the ordering financial institution has to ensure that all wire transfers carry specified information about the originator (Payer) who gives the instruction for the payment to be made and the Payee who receives the payment. The core requirement is that the Payer information consists of name, address, account number, official personal document number, customer identification number or date and place of birth; and that the Payee information consists of name and account number. There are also requirements imposed on any intermediary payment service providers.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The Companies (Prohibition of Bearer Shares) Act 2011 provides that bearer shares are not permitted as a form of ownership of legal entities and under the AML/CFT requirements, the existence of bearer shares in a non-Isle of Man incorporated entity should be considered as a risk factor.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

As per question 3.1, there is a wide range of businesses which have to comply with the Code. These include DNFBPs and so there are no other categories of business which have additional AML requirements.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

There is nothing additional for what is required under the primary legislation, the Code and associated guidance. It is important, however, to note that the Island has a range of Sanctions Notices in place in accordance with United Nations measures and the EU financial and economic sanctions. Isle of Man businesses are prohibited from doing business with any entity or individual named on a Sanctions Notice and must also be familiar with the conditions of doing business with sanctioned countries.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Consultation has been launched in February 2019 closing at the end of March 2019 in respect of changes to the Code. This is further action by the Isle of Man to meet the recommendations made by MONEYVAL in its report of 2017. The proposed changes to the Code are accompanied by a number of other proposed changes including the proposed Regulations referred to in question 2.8, changes to certain parts of the primary legislation and changes to the Designated Businesses (Registration and Oversight) Act 2015. There is also a separate Code being consulted on for not for profit organisations.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The most recent MONEYVAL Assessment in 2017 did not identify any significant areas of non-compliance with the FATF Recommendations. There were, however, some weaknesses identified in relation to effectiveness of the Island's AML/CFT regime. These included a lack of data to support the findings of the National Risk Assessment, a modest number of convictions and over reliance by the FSA on the use of remediation plans. The Cabinet Office is tasked with taking action to address these and the first follow-up report to MONEYVAL was submitted in July 2018. This was favourably received by MONEYVAL and a further follow up report is to be submitted by July 2019. It is pleasing that the EU recognised the work being undertaken by the Island to respond to its MONEYVAL report and did not include the Island on its list of countries with significant AML/CFT deficiencies as published in February 2019.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Please see question 4.2.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

A good summary is set out in Part 7 of the FSA's Handbook. This is available on the FSA's website and is in English. The Handbook contains a copy of the Code. Primary legislation is available from the Attorney General's Chambers website and it is also in English.

Sinead O'Connor

DQ Advocates Limited
The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: *+44 1624 626999*
Email: *Sinead@dq.im*
URL: *www.dq.im*

Sinead is Head of Regulatory & Compliance Services for DQ. She regularly advises on compliance with AML/CFT requirements and provides training to Boards of Directors and others across the financial services sector on their responsibilities under the Isle of Man's AML/CFT framework. Sinead has spoken in several jurisdictions around the world on AML/CFT and is a member of the Isle of Man AML/CFT Advisory Group. She also chaired one of the sector specific sub-groups for the purposes of the Island's National Risk Assessment.

Kirsten Middleton

DQ Advocates Limited
The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: *+44 1624 626999*
Email: *Kirsten@dq.im*
URL: *www.dq.im*

Kirsten is an associate within the corporate and commercial team.

Kirsten advises both domestic and international clients on a wide range of corporate and commercial matters. In addition, Kirsten has advised clients on data retention under local regulatory law, applications for licences under the Financial Services Act 2008 and compliance with international tax investigations and requests under Tax Information Exchange legislation.

Kirsten has a Master's in Law from Northumbria University which primarily focused on the concept of 'suspicion' and 'legal professional privilege' within Anti-Money Laundering legislation.

DQ Advocates is a leading Isle of Man based law firm with an international reach.

We offer a full range of legal, regulatory and compliance services to our local and global clients.

DQ are accessible, responsive and commercial with client-oriented strategies and goals. Our specialist lawyers are recommended as leading lawyers in *Chambers & Partners* and *The Legal 500*.

Japan

Nakasaki Law Firm

Ryu Nakazaki

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering is criminalised by Article 11 of the Act on Punishment of Organized Crimes and by other related acts. The authority to prosecute money laundering belongs to the prosecutors.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The elements for the offence of money laundering are:

(1) disguising facts pertaining to the sources, acquisition, or disposition of "Criminal Proceeds, Etc.", which means (a) criminal proceeds, (b) property that are acquired in exchange of criminal proceeds, and (c) commingled property including criminal proceeds;

(2) hiding of Criminal Proceeds, Etc.; or

(3) (i) acquiring shares or ownership of an entity to control such entity using Criminal Proceeds, Etc., and (ii) executing such shares or ownership to appoint or remove any director or other management member, or to change representative director or similar officer.

Accomplice and accessories to such crime are also punishable.

The predicate offences of criminal proceeds include a variety of crimes, including but not limited to, all crimes which may result in four years' (or more) imprisonment.

Yes, tax evasion crimes are predicate offences.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes, there is a provision of extraterritorial jurisdiction for the crime of money laundering (e.g. Article 3 of the Law on Control of Punishment and Crime Profits of Organized Crime).

Yes, money laundering of the proceeds of foreign crime is subject to punishment in Japan.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

(i) The National Police Agency ("NPA"), and (ii) the government agency supervising the applicable industry area (e.g. Financial Services Agency for the bank industry) are both responsible for making investigations and for imposing administrative penalties. And if the NPA judges that criminal sanction is appropriate, it will ask the prosecutors to prosecute the case.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is corporate criminal liability.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Five years' imprisonment and a 10 million yen fine.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is five years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes, enforcement is only at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Yes. The court administers forfeiture procedures.

All property that fall under any of the following may be confiscated:

(i) instrumentalities of predicate offence or money laundering (together the "Crime");

(ii) Proceeds of Crime, including remuneration for Crime ("Criminal Proceeds");

(iii) property that is acquired in exchange for Criminal Proceeds; or

(iv) property of corresponding value of Criminal Proceeds in cases where the Criminal Proceeds are commingled with other property.

There is no non-criminal confiscation nor civil forfeiture.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, but such cases are rare.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions regarding money laundering are resolved through judicial processes.

A reform of the Code of Criminal Procedure in 2018 has enabled a plea-bargain.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The "Act on Prevention of Transfer of Criminal Proceeds" ("AML Act") is the basic law that provides for anti-money laundering. For details of the AML Act, there is a cabinet enforcement order of the AML Act and for further details, there is an enforcement ordinance pertaining to the AML Act.

Financial institutions and DNFBPs are required to (i) conduct Customer Due Diligence ("CDD") measures, (ii) maintain records of CDD information and of transactions with customers, (iii) file Suspicious Transaction Report ("SAR") where applicable, and (iv) make sufficient efforts to implement internal control to combat money laundering.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes. Self-regulatory organisations including those of financial institutions and DNFBPs generally set forth additional requirements. For example, the Japan Federation of Bar Association implements a rule on AML measures to be taken by lawyers.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, they are.

2.4 Are there requirements only at national level?

Yes. There is no anti-money laundering requirements imposed at local government level. Please note, however, that some local governments, including prefectures, demand business entities not to transact with crime organisations and such (or in other words, anti-social forces).

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see question 1.4 regarding the government agencies responsible for the examination for compliance and enforcement of anti-money laundering requirements. With regard to publicly available examination criteria, there is no apparent criteria, but, pertaining to financial institutions, the Financial Services Agency has issued a guideline pertaining to AML/TF measures to be taken.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the Financial Intelligence Centre of the NPA ("FIC") is the FIU in Japan. The FIC publishes an annual report of the result of its analysis of money laundering activities in Japan.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitation for administrative enforcement actions. For criminal actions, the statute of limitations is three years.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum penalty under the AML Act for individual is imprisonment up to two years and a fine up to 3 million yen. The maximum penalty for a legal entity is a fine up to 300 million yen.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

It depends on the law regulating the business. For example, banks could be sanctioned under the Banking Act for violation of applicable laws including the AML Act. Possible sanctions include (i) cancellation of a licence, (ii) order for suspension of business, and (iii) order for rectification.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Penalties for violations can be both administrative/civil as well as subject to criminal sanctions.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

Process for assessment: Administrative sanctions are imposed by supervising authorities with prior notice and hearing, but fines cannot be imposed.

Process of collection of sanctions: No fine as administrative sanction.

Process of appeal of administrative decisions: One may file a request to review the administrative decision to the supervising authority itself under Article 6 of the Administrative Complaint Review Act. If the supervising authority does not change the decision, a lawsuit may then be filed to cancel such administrative decision under Article 8 of the same act.

a) Not all administrative decisions are made public.

b) This is very rare but has happened.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Financial institutions including banks, securities companies, insurance companies, lending businesses, fund transfer businesses, credit card issuing companies, and finance lease companies, among others, are subject to AML regulations, as well as DNFBPs including lawyers, accountants, real estate brokers, jewellery dealers, company service providers and such.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The cryptocurrency exchanges are subject to anti-money laundering requirements as cryptocurrency exchanges. Transactions as cryptocurrency exchanges are subject to anti-money laundering requirements just as other obliged entities. Please note that cryptocurrency exchanges registered in Japan basically do not interpret themselves as a money transmitter in relation with Japanese law, and therefore they basically judge that Japanese anti-money laundering regulations on wire transfer and money transmitters are not applicable to themselves.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes, compliance programmes are required (e.g. Article 11 of the AML Act, Article 355 of the Companies Act, Article 12-2 of the Banking Act).

The compliance programme is expected to include the following:

(1) training of its officers and employees;

(2) establishment of internal rules to ensure compliance with applicable laws and regulations;

(3) appointment of an officer who will be responsible for ensuring compliance with AML regulations (of Japan);

(4) requiring consent of the officer referred to in (3) for high risk transactions;

(5) analysing money laundering risks and making reports of the result of such analysis, and updating such reports from time to time;

(6) monitoring of CDD records and transaction information to detect suspicious activities;

(7) take measures to ensure that able and appropriate staffs are hired or allocated;

(8) conducting audits;

(9) implementing measures to keep the records of customers up to date; and

(10) implementing AML measures equivalent to those required under Japanese law at its overseas subsidiaries and branches.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There is a seven-year recordkeeping of the requirement for transactions for financial institutions and DNFBPs. There are some exemptions to this requirement, including an exemption for transactions pertaining to the transfer of property with a value equal to or less than 10,000 yen.

For reporting of large currency transactions, please see the answer to question 3.5.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Financial institutions need to submit various reports pursuant to the Foreign Exchange and Foreign Trade Act. For example:

- Article 55 provides for reports for cross-border payment (as described further in question 3.5);
- Article 55-3 and 55-4 provides for reports for capital transactions; and
- Article 55-7 provides for reports on foreign exchange operations.

However, most of these reports may be submitted by a financial institution, in aggregate form, on a monthly, quarterly or annual basis depending on the type of report.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

For cross-border funds transfer in the amount exceeding 1 million yen, the relevant financial institution must submit a "Statement of Overseas Wire Transfer" (Article 4 of the Act on Submission of Statement of Overseas Wire Transfers for Purpose of Securing Proper Domestic Taxation).

For cross-border payments or set-offs in the amount exceeding 30 million yen, the resident in Japan, that is either the payor or the payee, needs to submit a payment report to the government (Article 55 of the Foreign Exchange and Foreign Trade Act). Please note that if the payment is done through an office or branch in Japan of a

bank or fund transfer business, such report will be submitted through such financial institution.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

For high-risk transactions, enhanced CDD measures are necessary.

For other transactions, normal CDD measures will be necessary, provided that for certain statutory low-risk transactions, CDD is not required unless the transaction is suspicious or very abnormal.

(1) Normal CDD Measures

(i) Main Methods of Verification of ID for Face-to-Face Transaction (for Individual Customers):

(a) having a customer present a photo ID document;

(b) having a customer present two types of no-photo-IDs;

(c) having a customer present no-photo-ID, and delivering transaction-related documents with non-transferrable certified mail to the address on such ID (*); or

(d) having a customer present no-photo-ID, and delivering transaction-related documents to the address on such ID.

* Please note that starting from April 2020, additional requirements will be required to use this method (c).

(ii) Main Methods of Verification of ID for Non-Face-to-Face Transaction for Legal Entities

For a legal entity customer, the customer must present an ID document (e.g. certification of the commercial registry) of such legal entity or the obliged entity may conduct customer verification process by using the official commercial registry service or the corporation ID website operated by the National Tax Authority of Japan. About the verification methods of the representative of the customer, please see (i).

(iii) Main Methods of Verification of ID for Non-Face-to-Face Transaction for Individual Customer

(a) receiving a copy of ID document, and sending a non-transferrable certified mail to the address on such document;

(b) sending transaction-related document(s) to the customer's address and have an employee of the mail service business entity confirm the ID presented by the customer at the residence and receive information pertaining to statutory items from such employee; or

(c) having a customer send photo(s) or video including such customer's face and ID document using an application provided by the Obliged Entity.

(iv) Main Methods of Verification of ID for Face-to-Face Transaction for Legal Entities

For legal entity customers, method (a) of (iii) is possible. Also, the obliged entity may receive certification of commercial registry by electronic methods pursuant to statutory procedures, or may conduct customer verification process by using the official commercial registry service or the corporation ID website operated by the National Tax Authority of Japan.

Regarding the verification methods of the representative of the customer, please see (iii).

(v) Cases Where Verification of ID is Necessary

Transactions that require verification of ID ("Designated Transactions") are (x) transactions falling under any of the items provided for in Item 1, Article 7 or Article 9 of the Cabinet Order of the AML Act, and (y) suspicious or very abnormal transactions. Transactions falling under (x) include the opening of bank accounts, and payment of cash in the amount exceeding 2 million yen, among other various transactions.

For transactions falling under (x), there are some statutory exceptions (e.g. transactions with existing customers where verification of ID has been conducted before).

(vi) Other Items to be Verified

Other items to be verified include:

(a) the purpose of the transaction;

(b) identification of the agent and its authority as agent;

(c) occupation (in case of individual)/purpose (in case of legal entity); and

(d) identification of the substantial owner (in case of legal entity).

(2) Enhanced CDD Measures

(i) Extent of High-Risk Transactions

Statutory High-Risk Transactions are:

(a) Designated Transactions with Foreign Politically Exposed Persons ("Foreign PEPs");

(b) Designated Transactions with Residents of High-Risk Countries (which are currently Iran and DPRK); or

(c) transactions derived from a Designated Transaction in which Transaction ID fraud or ID theft is suspected.

(ii) Additional Requirements for High-Risk Transactions

For Statutory High-Risk Transactions, the following requirements need to be complied with in addition:

(a) verification of ID for Designated Transactions may not be abbreviated even if the customer ID has been verified before (*);

(b) verification of the identification of the substantial owner needs to be conducted by verifying statutory documents (e.g. shareholders registry, annual securities report); and

(c) verification of the asset and income of the customer is required if the transaction results in transfer of property in the amount exceeding 2 million yen.

* The additional requirement of (a) above is too burdensome and is heavily criticised. For example, even if a bank has verified the ID of a Foreign PEP customer when opening a bank account, the bank will have to confirm the ID of the customer every time the customer receives a loan from the bank using such account. The NPA is very strict on this. This restriction discourages financial institutions from having transactions with Foreign PEPs.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Establishment of a shell bank is not permitted in Japan.

Also, banks and fund transfer businesses licensed or registered in Japan are required to make investigations as to whether the financial institution that it will enter into a correspondent agreement with is a shell bank or not (Article 9 of the AML Act).

3.9 What is the criteria for reporting suspicious activity?

There are basically two types of transactions that are subject to the submission of SARs. One is transactions where the funds that the relevant financial institution or the DNFBP receives from the customer is suspicioned to be Criminal Proceeds, etc. The other is transactions where the customer is suspicioned to be engaging in

Money Laundering. Also, government agencies supervising each type of Obliged Entities usually issue examples of transactions that would require the filing of SARs.

Lawyers, accountants and similar professions are exempted from submitting SARs. They may submit SARs when they deem necessary, but they are not obliged to do so under Japanese law.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Japanese legal entities are registered in the commercial registry administered by the government. However, the name of shareholders will not be registered in the commercial registry.

When a legal entity registers certain items requiring shareholders resolution, including the appointment of corporate officers, the applicant will need to submit an attached document listing names of principle shareholders and other items to the registrar, and third parties may request to view such attached document, if such third party has special interest to such resolution. The Japanese government has shown an interpretation that the interest of financial institutions to conduct CDD appropriately may be considered in this respect, but the original purpose of such provision is not to facilitate CDD.

Thus, the commercial registry is imperfect for such purpose.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, for both questions (Article 10 of the AML Act); provided, however, that this Article seems to be interpreted not to apply basically to card transactions (e.g. through Visa and MasterCard), as described in the Interpretive Notes to FATF Recommendation 16.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Yes. The provision in the Companies Act referring to bearer shares has been abolished, but stating the name of the holder onto a share certificate is not obligatory (Article 216 of the Companies Act), so bearer shares do exist and are not prohibited.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No. The regulations are basically the same for financial institutions and DNFBPs.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

(1) In relation to the AML Act, the general rules for AML measures generally do not apply to lawyers and the rules of the Japan Federation of Bar Associations apply instead. This creates some difference, but it is not that significant.

(2) In relation to the Foreign Exchange and Foreign Trade Act, banks and funds transfer businesses are required to conduct CDDs when providing cross-border wire transfer or other funds transfer services to its customers.

Also, banks, securities companies, currency exchange businesses, and certain other types of financial institutions are obliged to conduct CDDs when providing services regarding certain cross-border capital transactions, including but not limited to loans, acceptance of deposits, and currency exchange. The CDD measures required under the Foreign Exchange and Foreign Trade Act are basically equivalent with the CDD measures required under the AML Act.

(3) Under tax related laws, banks and securities companies are basically required to ask the 'My Number' of the customer when opening an account, a social security and tax number given to each individual resident by the Japanese government. The customer is required to verify the My Number using My Number Card or My Number Notice held by such customer or by a copy thereof. Please note that the My Numbers need to be held in strict confidentiality.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

No proposal is publicised at this moment. However, after the FATF mutual evaluation report on Japan will be publicised (see question 4.3), I expect some amendment to the AML Act be enacted to implement changes that the FATF will recommend in such report.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Yes.

(1) Only wire transfer services and similar services (or *kawase torihki*) are regulated and other types of money transfer services are not required to register and are not subject to AML regulations.

(2) Electronic money and prepaid cards are not regulated by AML regulations.

(3) Acquiring of credit cards, prepaid cards, and debit cards are not subject to AML regulations.

(4) Finance lease, and currency exchange businesses are not subject to any permit, licence, authorisation nor registration requirements.

(5) Ongoing CDD measures are not required under the AML Act. For financial institutions, there is a provision in the AML guideline demanding such measures, but there is no such guideline for non-financial institutions.

(6) Transactions with "Domestic" Politically Exposed Persons are not high-risk transactions.

(7) Pachinko, which is one type of casino which can be found all over Japan, is not regulated by AML regulations.

(8) No provision of beneficial ownership for trusts.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes. The last review was in the year 2008 and the report can be

found at http://www.fatf-gafi.org/documents/documents/mutualevaluationofjapan.html.

The next mutual evaluation process is expected to start in the year 2019 and to end over the following year.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Laws, regulations and guidance can be found on the government website of Japan.

The English translation of Japanese laws in general can be found on the below website of the government. However, some laws or their most current versions are not translated, yet. Please see http://www.japaneselawtranslation.go.jp/?re=02.

The AML Act was on the above website, but has been amended and is not on the website any more.

The translation of the AML Act and Enforcement Ordinance of the AML Act, before amendment can be found at the below website of NPA, but the contents are not up to date:

https://www.npa.go.jp/laws/shokanhourei/hansyuu.pdf.

https://www.npa.go.jp/sosikihanzai/jafic/en/hourei_e/data/sekoukisoku2504.pdf.

Ryu Nakazaki
Nakasaki Law Firm
6th Floor, Toyo M Building, 1-9-7
Kudankita, Chiyodaku
Tokyo 102-0073
Japan

Tel: +81 3 6261 7500
Email: ryu@nakasaki-law.com
URL: www.nakasaki-law.com

Partner, Nakasaki Law Firm.

Mr. Nakazaki specialises in the areas of (i) finance (money transfer, loan, card business, AML, Fintech, etc.), and (ii) internet businesses (advertisement, data business, internet mall, online games, PII, IP, etc.). He assists clients in business collaboration agreements, licence agreements, and other transactions in the above areas and gives legal advice on regulations in Japan.

He is the author of "The Act on Prohibition of Criminal Proceeds and the Act of Foreign Exchange and Foreign Trade Act", "Instalment Sales Act" (the act regulating credit cards) and other books and is the Statutory Auditor of Japan Online Game Association (2015–2018).

Mr. Nakazaki has engaged in (i) the amendment of the credit card act (or the Instalment Sales Act), and (ii) the supervision of related regulations including AML as deputy director in the Japanese government.

Mr. Nakazaki has spent eight years in the U.S. (five years in New York and three years in California).

Nakasaki Law Firm

Nakasaki Law Firm was founded in 2018 and advises many clients including financial institutions (banks, credit card companies, insurance companies, Fintech companies), as well as internet business companies on various Japan-related laws, issues and transactions.

Kenya

Leah Njoroge-Kibe

JMiles & Co.

Elizabeth Kageni

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Proceeds of Crime and Anti-Money Laundering ("the Act") is the principal legislation and is supplemented by the Proceeds of Crime and Anti-Money Laundering Regulations ("the Regulations"). The Act and Regulations apply uniformly in the country both at national and county levels.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Section 3 of the Act provides that the prosecution needs to prove that the accused person entered into or became concerned in an engagement or arrangement, which he knew or ought to have known facilitated the acquisition, retention, use or control of criminal property (proceeds of crime) and by or on behalf of another person, the effect of which would conceal or disguise the source of the proceeds.

Anti-money laundering is considered a stand-alone offence as the Act adopts an all-crimes approach. The prosecution does not need to prove a predicate offence before laying charges for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes. Section 127 of the Act extends its application to the conduct of a person that takes place outside of Kenya which constitutes an offence under it, if the conduct would constitute an offence against a provision of any law in Kenya.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Section 122 of the Act mandates the office of the Attorney General to initiate investigations relating to money laundering offences. The Act also establishes the Financial Reporting Centre ("the Centre") as a regulatory authority intended to assist with the identification of proceeds of crime and combatting money laundering in compliance with international standards, and to collaborate with similar bodies in other countries regarding anti-money laundering efforts and related offences.

1.5 Is there corporate criminal liability or only liability for natural persons?

Yes. The Act imposes criminal liability for both natural and legal persons for (a) money laundering, (b) acquisition, possession or use of proceeds of crime, and (c) financial promotion of an offence.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Section 16 (a) and (b) of the Act provides for the penalties. In the case of a natural person, the Act provides that on conviction, a person is liable to imprisonment for a term not exceeding 14 years, a fine not exceeding Kshs. 5,000,000 or the amount of the value of the property involved in the offence, whichever is higher, or to both a fine and imprisonment. In the case of a body corporate, the offence is punishable with a fine not exceeding Kshs. 25,000,000 or the amount of the value of the property involved in the offence or whichever is higher.

1.7 What is the statute of limitations for money laundering crimes?

There is no limitation of actions for criminal offences. Money laundering is classified as a criminal offence and as such the Limitations of Actions Act does not apply.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

No. Enforcement applies uniformly at both national and county level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Yes. The Asset Recovery Agency is mandated by the Act to trace, freeze, seize and confiscate assets which are the proceeds of crime.

Monetary instruments being conveyed to or from Kenya which are suspected of being tainted property can be temporarily seized by authorised customs officers for not more than five days to enable them to obtain a court order.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

As at the date of this publication, as far as the authors are aware, cases against employees of banks and regulated financial institutions who have been charged under the Act are still ongoing.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions are resolved in court and hearings are open to the public. The Criminal Procedure Code, however, provides for plea arrangements. A plea arrangement can be initiated by the prosecutors or the accused person and this can only be raised after the accused person has been arraigned in Court. The contents of a plea arrangement are not public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The authorities include the Centre, whose function is to assist in the identification of the proceeds of crimes and the combatting of money laundering (s.21). The Act also provides for supervisory bodies specified in the First Schedule of the Act which report to the Centre. These bodies include: the Central Bank of Kenya; the Betting and Licencing Control Board; the Insurance Regulatory Authority; the Capital Markets Authority; the Institute of Certified Public Accountants of Kenya; the Estate Agents Registration Board; the Non-Governmental Coordination Board; and the Retirement Benefits Authority. The Act requires reporting institutions to comply with a wide array of obligations. The Act prescribes that reporting institutions shall monitor and report to the Centre complex, unusual, suspicious, or large transactions as they relate to money laundering and proceeds of crime. This includes filing reports of cash transactions that exceed US$10,000 (s.44). Financial institutions have an obligation to verify customer identity (s.45); establish and maintain customer records (s.46); and establish and maintain internal reporting procedures (s.47). There is also the requirement to keep the records for seven years. Reporting institutions must also register with the Centre (s.47A). The Act also authorises the Minister to issue regulations that require reporting institutions to fulfil various other obligations such as the implementation of compliance programmes, training of staff to recognise suspicious activities, implement internal procedures and to provide for an independent audit of its monitoring procedures. The Central Bank has issued further guidance on the Act, and requires, effective 31 December 2015, financial institutions to file two types of returns: a quarterly return to capture data on exposure of institutions to money laundering; and an annual self-assessment questionnaire to evaluate the systems of controls of an institution. This is according to the Central Bank of Kenya Banking Circular No. 1 of 2015 to CEOs of Commercial Banks, Mortgage Finance Companies and Microfinance Banks.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

The Institute of Certified Public Accountants of Kenya ("ICPAK") is the only professional association listed in the Act as a supervisory body, in that capacity, the staff of ICPAK are by law required to comply with the requirements of the Act. For instance, s.36 obliges staff of supervisory bodies to comply with reporting requirements under the Act. It is not clear, however, whether ICPAK's obligations under the Act extend to its members. The association undertakes compulsory continuous professional development courses for its members, for which training on anti-money laundering would be a key subject. The Central Bank of Kenya has put in place Prudential Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism which guides financial institutions when undertaking risk assessment.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

No. The sanctions provided for under the Act are enforced by the Centre.

2.4 Are there requirements only at national level?

No. The requirements apply at all levels.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

In addition to the Centre, the Act establishes the Anti-Money Laundering Advisory Board and the Asset Recovery Agency. These bodies are responsible for the compliance and enforcement of anti-money laundering requirements imposed by the Act. The supervisory bodies and reporting institutions report to the Centre on suspicious activity and the Centre takes appropriate action which includes forwarding information to law enforcement authorities. According to the Act, the Centre's powers were expanded to enable it to impose civil penalties for non-compliance with the obligations under the Act. Criminal sanctions are conducted by the relevant law enforcement agencies.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the Centre is the Financial Intelligence Unit under the Act. The Centre compiles statistics and records arising out of information received and also creates and maintains a database of suspicious transactions.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no time limitation period for authorities to bring enforcement actions. Money laundering is classified as a criminal offence and as such the Limitations of Actions Act does not apply.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

In addition to the identification, tracing, freezing, seizure and confiscation of the proceeds of crime, the Act provides that a person who fails to comply with its provisions will be liable to a monetary penalty not exceeding Kshs. 5,000,000. The penalty for a corporate body will not exceed Kshs. 25,000,000. In the case of continued failure, the person or reporting institution shall be liable to an additional monetary penalty of Kshs. 10,000 per day for a maximum of 180 days.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The Act gives powers to the Centre to take administrative action such as: (i) seek revocation of licences for financial and real estate institutions that are used as conduits for money laundering activities; (ii) issue warnings and directions to reporting institutions; (iii) bar persons from employment with reporting institutions; and (iv) issue an order to a competent supervisory authority requesting the suspension or revocation of a licence or registration of a specified reporting institution whether entirely or in a specified capacity or of any employee of the reporting institution (s.24C(1)). Apart from financial organisations, the powers of the Centre extend to non-governmental organisations, non-financial entities such as real estate agencies, those dealing in precious stones, casinos and certain professions such as accountants.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Yes. Violations of the Act are also subject to criminal sanctions although the offence is not prescribed in the Penal Code. The Assets Recovery Agency is responsible for implementing Parts VII to XII of the Act which covers applications for confiscation, seizure and forfeiture, among others. The Act specifies that such proceedings are civil in nature.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The Assets Recovery Agency is responsible for investigating and implementing the various sanctions against persons who have breached the Act. The Agency has powers to investigate and apply to the court to obtain orders for confiscation, forfeiture, restraint and preservation. An interested party affected by the orders issued by the court may apply for rescission of the orders. The orders of the court remain in force pending the outcome of any appeal against the decision concerned (s.97). The actions of the Agency pursuant to their powers of recovery of the proceeds of crime are generally public because the orders have to be issued by the court. In relation to the administrative actions conferred to the Centre under s.24C of the Act against a reporting institution, there is no indication whether these are publicly available. The Act only mentions that the Centre shall give a written notice to the relevant institution or person as to why the administrative action should not be taken. In addition, an aggrieved person can make an application for judicial review in the courts against an administrative decision, which if successful would overturn the decision of the Agency.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Section 2 of the Act provides that any person or entity, which conducts as a business, one or more of the following activities or operations is a financial institution:

(a) accepting deposits and other repayable funds from the public;
(b) lending, including consumer credit, mortgage credit, factoring, with or without recourse, and financing of commercial transactions;
(c) financial leasing;
(d) transferring of funds or value, by any means, including both formal and informal channels;
(e) issuing and managing means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money);
(f) financial guarantees and commitments;
(g) trading in money market instruments;
(h) transferable securities;
(i) commodity futures trading;
(j) participation in securities issues and the provision of financial services related to such issues;
(k) individual and collective portfolio management;
(l) safekeeping and administration of cash or liquid securities on behalf of other persons;
(m) otherwise investing, administering or managing funds or money on behalf of other persons;
(n) underwriting and placement of life insurance and other investment related insurance; and
(o) money and currency changing.

Designated non-financial business and professions include casinos (including internet casinos), real estate agencies, precious metals and stones dealers, accountants, non-governmental organisations or any other business in which the risk of money laundering exists as the Minister may, on the advice of the Centre, declare.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Cryptocurrencies are not considered legal tender in Kenya. Under the National Payments Act, 2011 the Central Bank is mandated to

identify and designate a national payment system. This Act and its Regulations do not recognise or regulate digital currencies such as Bitcoin. In fact, the Central Bank, in its Banking Circular dated 18 December 2015, issued a stern warning to local banks that digital currencies are not accepted as legal tender in Kenya, therefore no protection exists in the event the businesses or exchanges that hold the currencies fail. In tow, the Capital Markets Authority, Kenya's stock market regulator, has also issued warnings to the public against investing in transactions such as Initial Coin Offerings without its approval and the approval of the Central Bank of Kenya. In the circumstances, Kenya's anti-money laundering requirements have not at all dealt with the risks associated with the cryptocurrency industry. However, with increased interest from the public in cryptocurrency, there is perhaps scope in the near future for the Central Bank to issue guidelines on how it intends to apply anti-money legislation to deal with the cryptocurrency industry.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes. The Act requires the financial and designated non-financial businesses (collectively defined as reporting institutions) (a) to monitor and report on an ongoing basis all complex, unusual, suspicious, and large or such other transactions to the financial reporting centre, (b) to verify a customer's identity, (c) to establish and maintain customer records, and (d) to register with the Centre. Customer records shall be kept by the reporting institution for a period of at least seven years or such longer time as the Centre may prescribe.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Reporting institutions are required to file reports of all cash transactions exceeding US$ 10,000 or its equivalent within seven days of the transaction, whether they appear suspicious or not. Reports filed should include the following details: (a) the name, physical and postal address and occupation (or where appropriate business or principal activity) of each person (i) conducting the transaction, or (ii) on whose behalf the transaction is being conducted, as well as the method used by the reporting institution to verify the identity of that person; (b) the nature, time and date of the transaction; (c) the type and amount of currency involved; (d) the type and identifying number of any account with the reporting institution involved in the transaction; (e) if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument; and (f) the name and address of the reporting institution and of the officer, employee or agent of the reporting institution who prepared the record (s.46(2)).

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No. Reporting institutions are required to adhere to the Act and the Regulations specifically require reporting institutions to file reports with the Centre on all cash transactions equivalent to or exceeding US$ 10,000 or its equivalent in any other currency, whether or not the transaction appears to be suspicious.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes. However, the Act does not expressly provide for reporting requirements for cross-border transactions as it requires reporting institutions to monitor and report all transactions equivalent to or exceeding US$ 10,000. This requirement would therefore include cross-border transactions. The Act and the Regulations also require that cash declarations be made at any port of entry for any amounts equivalent to or exceeding US$ 10,000. The declarations are to be made to the customs officer who then makes a report to the Centre.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Reporting institutions are, under the Act, required to obtain full particulars of the customer's identity and have a sound knowledge of the purpose for which the customer is seeking to establish a business or relationship with the reporting institution. This applies to natural, juridical persons and government departments. Also, after the Act came into force, reporting institutions were required to conduct due diligence on existing customers or clients.

Under the Regulations, reporting institutions are required to formulate internal control measures and procedures for risk assessment which should include enhanced due diligence procedures for high risk persons, business relations and transactions. These procedures will also apply to persons established in jurisdictions that do not have adequate systems in place to combat money laundering. Reporting institutions are required to determine high risk persons or transactions from their internal procedures.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes. Section 25(1) of the Regulations prohibits reporting institutions from: (a) opening a foreign account with a shell bank; (b) permitting its accounts to be used by a shell bank; or (c) entering into or continuing a correspondent financial relationship with: (i) a shell bank; or (ii) a respondent financial institution that permits its account to be used by a shell bank.

3.9 What is the criteria for reporting suspicious activity?

The Act does not expressly provide for a criteria, however, reporting institutions are required to monitor on an ongoing basis all complex, unusual, suspicious, large or such other transactions as may be specified in the Regulations, whether completed or not, and shall pay attention to all unusual patterns of transactions, and to insignificant but periodic patterns of transactions which have no apparent economic or lawful purpose as stipulated in the

Regulations. In this case, suspicious activity is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence. Suspicious activity should be reported to the Centre immediately and in any event within seven days of the date of the transaction.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The government can obtain information about legal entities and their ownership structure (including beneficial ownership information) in three ways:

(1) By means of the register of members – through the amendments introduced to the Companies Act 2015, Companies (Amendment) Act 2017 all companies whether private and public are required to keep a register of beneficial owners (s.93 (1)) and lodge a copy of the register with the Registrar of Companies. The company has an obligation to update the register if there are any changes to the ownership structure within 14 days (s.93 (9)). However, there is no requirement to make the register of members available to authorities in a timely manner.

(2) Registrar of Companies – following on from the above provisions of the Companies Act, the register of members is open for inspection by the public (s.852) in the case of a public company. The companies' registry also maintains an online portal (e-citizen) where information on companies can be accessed by government agencies and financial institutions. There is the risk that such information may not be current as there is no requirement to provide this information to the authorities in a timely manner.

(3) Customer records – under the Act, the government can obtain customer records from reporting institutions pursuant to sections 44–47. Section 46 imposes a requirement to provide the information to competent authorities in a timely manner. The 2017 amendments in relation to beneficial ownership are not yet functional, however, when they do become functional, they should extend the scope of information to be recorded in the register of members to capture more information that would be relevant to anti-money laundering agencies.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes it is. The Regulations at s.27 require that when conducting wire transfers reporting institutions must always include information about the originator and beneficiary. The Central Bank Prudential Guidelines issued in 2013, at 5.6.8.1 provides that for wire transfers, information about originators and beneficiaries should be included in payment orders for a funds transfer. The information applies to institutions in circumstances where the institution is acting as an ordering financial institution and as a beneficiary financial institution.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Bearer shares are prohibited by s.504 of the Companies Act of 2015 (revised in 2017).

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

The Act designates non-financial institutions and professional associations as reporting institutions whose obligations are outlined in the Act and in the 2013 Regulations. In that regard, non-financial institutions and businesses are required by s.12 of the Act to report to the Centre all conveyance of monetary instruments in excess of US$ 10,000.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

There are no specific anti-money laundering requirements that apply to persons engaged in international trade or free zones. There are, however, guidelines in relation to mobile money payments. The CBK issued the Anti-Money Laundering Guidelines for the Provision of Mobile Payment Services of 2013, under its mandate conferred to it by s.3 of the National Payment Systems Act. The purpose of the guidelines is to define the anti-money laundering requirements for the delivery of mobile payment services and implement and enforce anti-money laundering legislation for mobile payment systems. It also aimed to ensure that mobile payment service providers are compliant with the anti-money laundering legislation.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

In relation to beneficial ownership, the Office of the Attorney General is considering amendments to the Companies Act 2015 to prohibit the use of nominee shareholders and directors. Further amendments to the Companies Act also include the removal of s.104 (1) which states that "a company shall not accept, and shall not enter in its register of members, notice of any trust, expressed, implied or constructive". In its 2017 publication, *Towards Beneficial Ownership Transparency in Kenya an Assessment of the Legal Framework*, Transparency International Kenya notes that this section of the Companies Act contradicts the requirement for companies to maintain a register of members including beneficial owners, see question 3.9 above.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Kenya has made significant strides in combatting money laundering since the entry into force of the Proceeds of Crime and Anti-Money Laundering Act of 2009, the provisions of which largely model the FATF recommendations. The Act provides the Centre with enforcement powers to impose civil sanctions for breaches under the Act and to take more stringent administrative actions. Challenges with compliance to the FATF recommendations lie principally with the law enforcement agencies and particularly the Centre, which is currently under-resourced.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Kenya is a member of the Eastern and Southern Africa Anti-Money Laundering Group ("ESAAMLG") which in turn is a member of the FATF. ESAAMLG conducted its evaluation of Kenya's anti-money laundering regime in 2011 which rated Kenya's compliance with the FATF recommendations. The next review will be conducted in 2020–2021.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

All relevant anti-money laundering laws are available in English and are online. The following are links from the internet where one can download the anti-money laundering laws and regulations:

http://frc.go.ke/downloads/category/2-acts-and-regulations.html.

http://kenyalaw.org/lex/rest/db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/C/Companies%20Act%20-%20No.%2017%20of%202015/docs/CompaniesAct17of2015.pdf.

https://www.centralbank.go.ke/wp-content/uploads/2016/08/PRUDENTIAL-GUIDELINES.pdf.

Leah Njoroge-Kibe

JMiles & Co
5th Floor, The Oval
Junction of Ring Road Parklands and
Jalaram Road, Westlands
Nairobi
Kenya

Tel: +254 20 434 3159 / +254 700 000 106
Email: lnk@jmilesarbitration.com
URL: www.jmilesarbitration.com

Leah Njoroge-Kibe is a Senior Associate at JMiles & Co. She is a Kenyan-qualified lawyer who specialises in international arbitration, negotiation and dispute settlement. She has an extensive background in international law and economics, international trade law, WTO law, international investment law, preferential/regional trade agreements, bilateral agreements and international public law. Leah has a Master's Degree in International Law and Economics from the World Trade Institute in Switzerland and has worked in the Division of Investments and Enterprise of the United Nations Conference on Trade and Development ("UNCTAD") in Geneva. Leah frequently speaks on trade and investment topics and most recently presented on Investor State Dispute Settlement at a workshop organised by the Commonwealth Secretariat in Nairobi. Leah is the regional representative for Kenya for LCIA YIAG and Africa representative for the Asia-Pacific Forum on International Arbitration ("AFIA").

Elizabeth Kageni

JMiles & Co
5th Floor, The Oval
Junction of Ring Road Parklands and
Jalaram Road, Westlands
Nairobi
Kenya

Tel: +254 700 000 106 / +254 20 434 3159
Email: ek@jmilesarbitration.com
URL: www.jmilesarbitration.com

Elizabeth is an Associate at JMiles & Co. Elizabeth specialises in international arbitration, negotiation and dispute settlement, investigations and advisory work. She has an extensive background in corporate and commercial law, real estate and finance and civil litigation in Kenya.

JMiles & Co.
Arbitration • Investigation • Consultancy

JMiles & Co. is an international legal consultancy, based in Nairobi Kenya. JMiles& Co provides bespoke services in the areas of international arbitration, fraud investigations and asset chasing, investment consulting, and mediation.

The JMiles Team consists of lawyers who have qualified and practised in England & Wales, Kenya and Singapore, all with a wide knowledge of Africa. The team offers sound legal advice and has a deep understanding of the legal and commercial realities of the continent. The firm has worked consistently with African governments and international corporations both on the continent and elsewhere across the world.

Liechtenstein

Laura Vogt

Julia Pucher

Marxer & Partner Attorneys at Law

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The crime of money laundering like almost all other criminal offences (except some minor misdemeanours which are only prosecuted upon request by the injured private party) is prosecuted by the Liechtenstein public prosecutor's office.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The Liechtenstein Criminal Code (hereinafter: StGB) distinguishes between money laundering with respect to assets originating from a criminal offence (§ 165 (1) and (2) StGB) and money laundering with respect to assets belonging to a criminal organisation or a terrorist group (§ 165 (6) StGB).

For a conviction pursuant to § 165 (1) or (2) StGB, the public prosecutor's office must prove that the perpetrator committed one of the punishable acts listed in § 165 para 1 StGB (hiding, concealing the origin, providing false information in legal transactions with regard to the origin/true nature/ownership/location) or § 165 (2) StGB (appropriating, taking into safekeeping, investing, managing, converting, realising, transferring to a third party) with respect to assets originating from one of the predicate offences exhaustively enumerated in the law. Furthermore, it must prove that the perpetrator acted with intent ("*dolus eventualis*") meaning that the perpetrator at least seriously considered the assets to be possibly originating from a crime and accepted this fact. If the predicate offence in question is tax fraud (Art 140 of the Tax Act), "*dolus eventualis*" is not sufficient within the scope of § 165 (2) StGB. Instead, the public prosecutor's office has to prove that the perpetrator knew that the assets concerned originate from tax fraud.

According to Liechtenstein law, predicate offences are all crimes (offences with a maximum penalty of more than three years of imprisonment) and the following misdemeanours: forgery of documents (§§ 223 f StGB); participation in a criminal association (§ 278 StGB); terrorist financing (§ 278d StGB); all forms of active and passive bribery (§§ 304 – 309 StGB); illegal residence (Art 83 of the Foreigners Act); furtherance of illegal residence/entry (Art 84 of the Foreigners Act); production or use of false identity papers or illegal use or transfer of authentic identity papers (Art 85 of the Foreigners Act); all misdemeanours according to the Narcotics Act; tax fraud (Art 140 of the Tax Act); and tax fraud and qualified tax evasion with respect to value-added tax (Art 88 f of the Value Added Tax Act). Finally, an infraction pursuant to Art 24 of the Market Abuse Act (market manipulation) can be a predicate offence. Ordinary tax evasion is not a predicate offence.

For a conviction pursuant to § 165 (6) StGB, the public prosecutor's office must prove that the perpetrator appropriated or took into safekeeping assets of a criminal organisation or a terrorist group on behalf of or in the interest of a criminal organisation or terrorist group. Furthermore, it must prove that the perpetrator acted with intent ("*dolus eventualis*").

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The Liechtenstein Criminal Code is applicable and Liechtenstein law enforcement authorities competent if either the predicate offence (*cf.* § 64 (1) (9) StGB) or the punishable act constituting money laundering (i.e. the concealing, the management … *cf.* § 62 StGB) was committed in Liechtenstein. In the latter case, it is irrelevant where the predicate offence was committed. Furthermore, it is noticeable that proceeds of foreign crimes which are not subject to the jurisdiction of Liechtenstein can be forfeited and confiscated if only the crime is punishable according to the law of the state in which the crime was committed (*cf.* § 65a StGB).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

In principle, the public prosecutor's office is responsible for investigating and prosecuting money laundering criminal offences. The public prosecutor's office may, however, instruct the police or the investigating judge to conduct measures of investigation (e.g. interrogations, assets transfer analysis…). The police are also entitled to conduct measures by their own if they become aware of a suspicion that a criminal offence was committed. If, however, the suspicion concerns a serious offence or an offence which raises particular public interest, the public prosecutor's office has to be informed immediately. In any event, the police have to inform the public prosecutor's office at the latest three months after the first investigation measure against a specific person was taken.

1.5 Is there corporate criminal liability or only liability for natural persons?

The Liechtenstein Criminal Code provides in general for corporate criminal liability and not only with respect to specific criminal offences. The law distinguishes between underlying acts committed by managers and underling acts committed by "ordinary" employees. According to § 74a (1) StGB, legal entities are liable for any misdemeanours and crimes committed unlawfully and culpably by managers in the performance of business activities and within the framework of the purpose of the legal entity (except if the managers are acting in enforcement of the laws). In contrast, according to § 74a (3) StGB, legal entities are only liable for misdemeanours and crimes committed unlawfully (but not necessarily culpably) by "ordinary" employees if the act was made possible or was significantly facilitated by the failure of the managing staff to take the necessary and responsible measures to prevent such misdemeanours or crimes.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The Liechtenstein Criminal Code provides for different penalties depending on the specific act of money laundering committed (active concealing of the proceeds of crimes according to § 165 (1) StGB *vs.* commonplace activities such as a simple storage of the proceeds of crimes according to § 165 (2) StGB) and depending on the amount of assets laundered.

If the crime of money laundering is committed with respect to an amount exceeding CHF 75,000, the penalty provided for by law for an individual is between six months of imprisonment and five years of imprisonment irrespective of the specific act committed. For legal entities, the maximum penalty in these circumstances is a monetary penalty of CHF 1,500,000 (up to 100 daily penalty units of a maximum of CHF 15,000). The same maximum penalties apply if the crime of money laundering was committed by a member of a criminal group that has been formed for the purpose of continued money laundering.

If the amount of assets concerned by the crime of money laundering does not exceed the threshold of CHF 75,000 and the crime of money laundering was not committed by a member of a criminal group, the penalty is up to three years of imprisonment (active concealing of the proceeds of crimes), respectively, up to two years of imprisonment (commonplace activities such as a simple storage of the proceeds of the crimes) or a monetary penalty up to CHF 360,000 (up to 360 daily penalty units of maximum CHF 1,000) for individuals. For legal entities, the maximum penalty is in these circumstances a monetary penalty of CHF 1,275,000 (up to 85 daily penalty units of a maximum of CHF 15,000), respectively, CHF 1,050,000 (up to 70 daily penalty units of a maximum of CHF 15,000).

1.7 What is the statute of limitations for money laundering crimes?

According to § 57 (3) StGB, the statute of limitations for money laundering crimes is five years. However, if, during the limitation period, the perpetrator commits another offence that arises from the same harmful inclination, the limitation period is prolonged until the limitation period has also expired for the second offence.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Liechtenstein has only two electoral districts, but no states or provinces. Therefore, there is only enforcement at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

In Liechtenstein, there are no special forfeiture or confiscation authorities. It is up to the Liechtenstein's prosecutor's office to ask the criminal court for a forfeiture or confiscation.

Any property used or intended to be used to commit an intentional criminal offence as well as all goods originating from committing an intentional criminal offence can be confiscated if, at the time of the decision of the criminal court, the perpetrator is the sole owner (*cf.* § 19a StGB).

Furthermore, pursuant to § 20 (1) and (2) StGB, all assets received for committing a punishable act as well as all assets obtained through a punishable act, including their profits and substitute values, can be forfeited. If the assets subject to forfeiture according to § 20 (1) and (2) StGB are no longer present or a forfeiture impossible for other grounds, the criminal court may forfeit an amount of money equivalent to these assets (*cf.* § 20 (3) StGB). In addition, the criminal court may also forfeit the amount of money the perpetrator has saved in expenses by committing the punishable act.

§ 20a StGB provides for certain exceptions in which a forfeiture is excluded despite the fact that the conditions according to § 20 StGB are met. In particular, forfeiture is excluded when a third party who has acquired the assets in question in return for payment without knowing about the punishable act is involved.

Pursuant to § 20b StGB, it is also possible to forfeit assets which are under the control of a criminal organisation or a terrorist group or which have been provided or collected for the financing of terrorism (so-called "extended forfeiture"). If a crime (any criminal offence with a maximum penalty of more than three years of imprisonment) has been committed for which or by which assets have been obtained, any other assets obtained in a temporal connection with the crime committed are subject to forfeiture if there is reason to believe that they were derived from an unlawful act and if their lawful origin cannot be credibly shown. If one of the following misdemeanours (money laundering, criminal association, terrorist offence or active/passive bribery) has been committed in a continuous or repeated manner for which or by which assets have been obtained, any other assets obtained in a temporal connection with these acts shall also be subject to forfeiture if there is reason to believe that they were derived from further misdemeanours of this kind and if their lawful origin cannot be credibly shown.

Finally, pursuant to § 26 StGB, all objects used by the perpetrator or intended by the perpetrator to be used to commit the punishable act and all objects obtained from the punishable act are subject to a deprivation order if these objects endanger the safety of persons, morality or the public order.

A forfeiture (§ 20 StGB), an extended forfeiture (§ 20b StGB) or a deprivation (§ 26 StGB) is also possible if there has been no criminal conviction. If the public prosecutor believes that there are sufficient reasons to assume that the preconditions for forfeiture,

extended forfeiture or deprivation are met and if is not possible to decide on this in criminal proceedings, the prosecutor can submit a separate application for the issuing of such pecuniary order.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Based on the publicly available information, no convictions of banks or other regulated financial institutions have occurred. However, it is publicly known that a (former) vice director of a bank and other employees of banks, respectively, regulated financial institutions who have been convicted of other crimes such as fraud or embezzlement have also been convicted of laundering the proceeds of their own crimes.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The Liechtenstein Criminal Procedure Code (hereinafter: StPO) does not provide for the opportunity to conclude settlements between the public prosecutor's office and a perpetrator. Thus, in general, criminal actions are only resolved through the judicial process. However, the public prosecutor's office can under certain circumstances refrain from filing charges against a perpetrator even though it realises sufficient grounds of suspicion.

According to §§ 22a ff StPO, the public prosecutor shall withdraw from the prosecution of a punishable act if, in view of the payment of an amount of money, the performance of community service, the setting of a probation period or a victim-offender-mediation, punishment does not seem advisable as a means to prevent the suspect from committing punishable acts or for counteracting the commission of punishable acts by others. In addition, the withdrawal from prosecution requires that (i) the punishable act constitutes an offence explicitly listed in § 22a (2) StPO, (ii) the suspect's level of culpability would not have to be considered grave, and (iii) the offence has not caused the death of a human being. With respect to money laundering, a withdrawal from the prosecution according to §§ 22a ff StPO is only possible if the threshold of CHF 75,000 is not exceeded and the crime was not committed by a member of a criminal group.

Such withdrawals from the prosecution are not public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

It is the Liechtenstein legislative authority (i.e. the Liechtenstein parliament called "Landtag" and the prince who must approve every law passed by parliament) who imposes anti-money laundering requirements on financial institutions and other businesses. It has done so by enacting the Due Diligence Act (hereinafter: SPG). The Liechtenstein Government has concretised some of the ant-money laundering requirements already provided for by the SPG in the Due Diligence Ordinance (hereinafter: SPV). Finally, the Liechtenstein Financial Market Authority and the Liechtenstein FIU have issued guidelines, communications and instructions with respect to anti-money laundering requirements.

For the details of these anti-money laundering requirements, please see the responses to section 3 (in particular question 3.1).

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

No, there are not.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The Liechtenstein Chamber of Lawyers is the only professional association which is responsible for anti-money laundering compliance and enforcement against their members. With respect to all other financial institutions and businesses subject to due diligence requirements, the Liechtenstein Financial Market Authority (FMA) is responsible for anti-money laundering compliance and enforcement.

2.4 Are there requirements only at national level?

As Liechtenstein is a small state, there are only requirements at national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The Liechtenstein Financial Market Authority (FMA) is responsible for compliance and enforcement of anti-money laundering requirements (with the exception of lawyers for which the Liechtenstein Chamber of Lawyers is solely competent). The FMA as well as the FIU (with respect to suspicious transaction reports) have issued guidelines which show how they construe the provisions of the SPG and the SPV in practice. Furthermore, the FMA publishes an annual report about its activity as well as a brochure called "FMA-Praxis" once a year, in which it informs about its own relevant decisions, relevant decisions of the FMA Complaints Commission, relevant decisions of the administrative court and relevant decisions of the constitutional court in anonymised form.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, there is. The Liechtenstein FIU is competent for analysing any suspicious transaction report received by a financial institution or other business subject to due diligence requirements. In the event of a reasonable suspicion of money laundering, predicate offences to money laundering, organised crime or terrorist financing, it has to file a report with the Liechtenstein public prosecutor's office containing the analysis and any other additional relevant information. The report to the Liechtenstein public prosecutor's office may not contain any details about the source of the information or disclosure.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

With respect to penalties, the limitation period is three years. For all other supervisory measures, the law does not provide for an explicit limitation period.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum penalty for failure to comply with anti-money laundering requirements is six months of imprisonment or a monetary penalty up to CHF 360,000 (up to 360 daily penalty units of maximum CHF 1,000), respectively, a fine up to CHF 200,000 (for administrative infractions which are prosecuted and judged by the FMA and not the public prosecutor's office, respectively, the criminal court). In case of serious, repeated or systematic violations, the fine for administrative infractions can be raised up to CHF 5,000,000, respectively, up to 10% of the annual total turnover (whichever amount is higher). For some of the businesses subject to due diligence obligations, the maximum fine is CHF 1,000,000, respectively, double the amount gained through the administrative infraction (whichever amount is higher).

Subject to penalty are any failures with respect to suspicious transaction reports (i.e. violating the reporting requirement, carrying out suspicious transactions before filing the report or carrying out suspicious transactions without ensuring the paper trail, informing third parties about the suspicious transactions reports and not freezing assets in case of a suspicion of terrorist financing). Furthermore, it constitutes a criminal infringement not to provide the FIU information requested according to the law or to provide false information to the FIU.

Almost every intentional failure of anti-money laundering obligation provided for by the SPG constitutes an administrative infraction (the list in the SPG is more than two pages long).

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The supervisory authorities may prohibit the commencement of new business relationships for a limited period of time and they may request the competent authority to undertake appropriate disciplinary measures. Furthermore, in the event of repeated, systematic or serious violations, the supervising authorities may (i) publicly disclose decisions against a financial institution or business subject to due diligence requirements (including the name of the infringer), (ii) temporarily prohibit the performance of the activity it has authorised under special legislation, (iii) withdraw the licence it has granted under special legislation, or (iv) temporarily prohibit members of the executive body and other natural persons from performing the executive functions it has authorised or taking up such functions yet to be authorised.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

The penalties are not only administrative. All violations of requirements with respect to suspicious transaction reports constitute criminal misdemeanours, respectively, criminal infractions which fall in the competence of the criminal court.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? A) Are all resolutions of penalty actions by competent authorities public? B) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

When imposing the penalties, the criminal court, respectively, the supervisory authorities must take into account the principle of proportionality and the principle of efficiency. Decisions of the criminal court can be appealed within 14 days to the court of appeal (the StPO applies). Decisions of the FMA can be appealed within 14 days to the FMA Complaints Commission and afterwards to the administrative court. Decisions of the Liechtenstein Chamber of Lawyers can only be appealed to the administrative court. Final decisions by the FMA or the Liechtenstein Chamber of Lawyers as well as final decisions by the criminal court constitute executory titles which can be enforced.

Pursuant to Liechtenstein law, not all decisions taken by the FMA (or the criminal court) are public. The decisions of the FMA are only published in case of serious, systematic or repeated violations. But even in this case, the FMA may refrain from the publication or only publish the decisions in anonymised form, e.g., for reasons of proportionality. Having said that, the FMA informs about its activities and decisions in annual reports and in brochures ("FMA-Praxis") in anonymised form. Decisions of the criminal court are only made public if considered relevant by the courts.

Yes, it is publicly known that penalty decisions (at least of criminal courts) have been appealed by financial institutions.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The following persons are subject to due diligence (e.g. anti-money laundering requirements):

- banks and investment firms;
- e-money businesses;
- undertakings for collective investment that market their unit certificates or units;
- insurance undertakings;
- the *Liechtensteinische Post Aktiengesellschaft*, insofar as it pursues activities beyond its postal service that must be reported to the FMA;
- exchange offices;
- insurance brokers;
- payment service providers;
- asset management companies;
- service profilers for legal entities;
- casinos and provider of online gaming;
- lawyers and law firms (insofar as they provide tax advice or assist in the planning and execution of financial or real estate transactions);
- members of tax consultancy professions and external bookkeepers;

- real estate agents; and
- persons trading in goods, insofar as payment is made in cash and the amount involved is 10,000 francs or more, irrespective of whether the transaction is executed in a single operation or in several operations which appear connected.

Such persons shall perform the following duties taking a risk-based approach:

- identification and verification of the identity of the contracting party;
- identification and verification of the identity of the beneficial owner;
- identification and verification of the identity of the recipient of distributions from legal entities established on a discretionary basis and the beneficiary of life assurance policies and other insurances with investment-related objectives;
- establishment of a business profile; and
- supervision of business relationships at a level that is commensurate with the risk.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

There are (so far) no special requirements in relation to the cryptocurrency industry included in the SPG.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

The persons subject to due diligence shall keep a record of compliance with the duties of due diligence and the reporting requirements as provided in the SPG.

They shall establish and maintain due diligence files. In these files, client-related documents, business correspondence and vouchers are to be retained for 10 years from the end of the business relationship and/or from execution of an occasional transaction, whereas transaction-related documents, business correspondence and vouchers shall be retained for 10 years from conclusion of the transaction and/or from their issue.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

In relation to record-keeping requirements, please see question 3.3 above.

There is no reporting requirement in relation to a threshold. However, any suspicion in relation to money laundering has to be reported immediately (see also the answer to question 3.9).

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, see above the answer to question 3.4.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes, the cross-border transactions reporting requirements apply to all financial intermediaries operating across borders.

Reporting has to be done in connection with legal and reputational risks arising from cross-border business activities. The Financial Market Authority (FMA) has to be informed in cases of substantial significance.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

When embarking upon a business relationship or concluding an occasional transaction, the person subject to due diligence shall establish the identity of the contracting party and verify that identity by consulting a supporting document (original or certified copy) relating to the contracting party and obtaining and recording the following details:

a) for natural persons: last name; first name; date of birth; residential address; state of residence and nationality; and

b) for legal entities: name or company style; legal form; address of registered office; state of domicile; date established; place and date of entry in the Commercial Register, where applicable; and the names of the bodies or trustees acting formally on behalf of the legal entity in the relationship with the person subject to due diligence.

With regard to business relationships and transactions with politically exposed persons, enhanced due diligence requirements have to be applied.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Correspondent bank relationships with shell banks are prohibited according to the SPG.

3.9 What is the criteria for reporting suspicious activity?

Where suspicion of money laundering, a predicate offence to money laundering, organised crime, or terrorist financing exists, the persons subject to due diligence must immediately report to the Financial Intelligence Unit (FIU) in writing.

The person subject to due diligence shall verify the plausibility of each customer statement to the best of its ability. If investigations reveal that the transactions or circumstances are implausible, this will trigger the reporting requirement.

The indicators of money laundering, organised crime and financing of terrorism are listed in Annex 3 of the SPV.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, in Liechtenstein a commercial register exists, which is open to the public and constitutes conclusive evidence. Moreover, a new register in relation to beneficial owners is currently being implemented.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

The payment order contains the name, account number and address of the payer as well as the name and account number of the beneficiary.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

It is only permitted if a custodian has been appointed and the issued bearer shares are deposited with the custodian. The custodian must be entered in the commercial register stating his function. The custodian has to keep a register in which each bearer, who has to be identified by the custodian in accordance with the law (Art 326c PGR), is entered. The person entered into the register is considered as shareholder. The result of the legal provisions is that the bearer is identified and documented in accordance with the rules of the due diligence legislation (SPG).

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the financial institutions and other businesses that are subject to anti-money laundering requirements are mentioned under question 3.1.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

The SPG applies to various business sectors and, in particular, also applies to persons trading in goods (see question 3.1 above). However, there are no requirements in relation to free trade zones, because in Liechtenstein there are no free trade zones or other special geographic areas.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

The Liechtenstein parliament has passed a new law which provides for a register of the beneficial owners of domestic legal entities in December 2018. This register shall be kept by the Office of Justice for the sole purpose of combatting money laundering, predicated offences of money-laundering and terrorist financing. The law has not yet entered into force (presumably on August 1, 2019).

Furthermore, it is planned to revise § 165 StGB establishing the offence of money laundering. The list of predicate offences shall be extended (in particular, all offences which have a maximum penalty of more than one-year of imprisonment shall be predicate offences). In addition, the maximum penalty shall be raised if the crime of money laundering is committed by a member of a criminal association or with respect to assets exceeding the amount of CHF 75,000 (from a maximum penalty of five years to a maximum penalty of 10 years which will also have the effect that the limitation period will be extended). Finally, the law shall explicitly provide that it is also possible in the future to commit the crime of money laundering with respect to expenses saved by a tax offence. The revision will presumably enter into force on July 1, 2019.

Lastly, the Criminal Procedure Code shall be revised insofar as judgments in absence of the perpetrator shall be possible not only with respect to misdemeanours (penalty up to three years of imprisonment), but also with respect to money laundering in cases in which it constitutes a crime (penalty of more than three years of imprisonment).

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

According to the last evaluation report by Moneyval (dated April 2, 2014), the legal framework as such is closely in line with the FATF recommendations. However, the effective implementation was criticised. In particular, it was criticised that there has only been one conviction of money laundering in the period between 2007 and 2014.

After the release of this evaluation report, Liechtenstein has undertaken several changes in legislation to facilitate enforcement of the anti-money laundering regime. Since 2014, there have been 27 final convictions of money laundering. As the next evaluation by Moneyval will not take place before 2020, it is unknown how the different changes in legislation are assessed by independent organisations.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes, the last on-site visit by Moneyval was in June 2013.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The relevant anti-money launderings laws are publicly available on www.gesetze.li (only in German) or – alternatively – on www.fma-li.li. The FMA provides English translations of the most relevant laws. They are, unfortunately, not always up-to-date. The FMA also publishes its guidelines, instructions and communications on its website (a few of them in English).

Criminal court decisions are available on www.gerichtsentscheidungen.li (in German only). The FMA publicly informs about its activity and its decisions in annual reports (available in English and in German) and brochures "FMA-Praxis" (available only in German).

Laura Vogt
Marxer & Partner Attorneys at Law
Heiligkreuz 6
9490 Vaduz
Liechtenstein

Tel: +423 235 81 81
Email: laura.vogt@marxerpartner.com
URL: www.marxerpartner.com

Laura Vogt, born in 1990, studied law at the University of Lucerne and Northwestern Pritzker School of Law (student exchange programme). She joined Marxer & Partner Attorneys-at-Law in 2014 and passed the Bar exam in 2017. She is part of the litigation team at Marxer & Partner Attorneys-at-Law.

Julia Pucher
Marxer & Partner Attorneys at Law
Heiligkreuz 6
9490 Vaduz
Liechtenstein

Tel: +423 235 81 81
Email: julia.pucher@marxerpartner.com
URL: www.marxerpartner.com

Julia Pucher, born in 1987, studied law at the University of Innsbruck. She received an LL.M. degree from the University of Zurich in 2016 where she joined a special programme on Banking and Finance. In 2018 she graduated as a Fiduciary Expert from the University of Liechtenstein. Before joining Marxer & Partner Attorneys-at-Law, in 2018 she worked as Deputy Head of the Automatic Exchange Division for the International Department of the Liechtenstein Fiscal Authority. As an expert in the field of Automatic Exchange of Information, she repeatedly represented the Liechtenstein delegation in various OECD working groups.

MARXER & PARTNER

RECHTSANWÄLTE

Marxer & Partner Attorneys-at-Law was very much involved in shaping Liechtenstein as a financial centre and has been growing with it. Established in 1925, it is the oldest and largest law firm in Liechtenstein, having 14 partners, four of-counsels, 12 associates and a supporting staff of about 50 paralegals and administrative specialists. Of all firms providing legal services to a demanding international clientele, Marxer & Partner has certainly become the most renowned in Liechtenstein.

For many years Marxer & Partner has focused its activities on the fields of corporate law, M&A, trust and estate planning, and capital markets, as well as tax. The firm provides in-depth knowledge and excellent advice in these fields to its international client base. Together with its auxiliary trust, management and auditing companies, Marxer & Partner form a centre of excellence that can handle all sorts of issues in financial, legal, tax, business management, and real estate affairs.

The firm represents Liechtenstein exclusively at Lex Mundi, the worldwide association of independent law firms.

Macau

Pedro Cortés

Rato, Ling, Lei & Cortés – Advogados

Óscar Alberto Madureira

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Under Macau SAR Basic Law, the entity with powers to coordinate criminal investigations and to prosecute money laundering (and any other) crimes is the Public Prosecutor's Office. Under the separation of powers principle prevalent in Macau under the Basic Law, the Public Prosecutor is classified with the judiciary power which, together with the legislative power, is independent and autonomous from the executive power, i.e. the Macau SAR Government.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Under applicable Macau regulations, those who convert or transfer benefits obtained by themselves or by third parties, or help or facilitate any of these operations in order to conceal its illicit origin or to prevent the perpetrator or participant in the crimes giving rise to them from being prosecuted or subjected to a penal reaction, practise a crime of money laundering punishable with an imprisonment penalty. That said, the prosecution will have to demonstrate in court the fulfilment of the necessary requirements in order to obtain the relevant conviction from the Court.

Tax evasion is not considered as a predicate offence for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Law 3/2017, which amended Law 3/2006, establishes the same rules for facts or acts which took place overseas. The same applies to money laundering of the proceeds of foreign crimes, which are also punishable.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Under Macau SAR Basic Law, the entity with powers to coordinate criminal investigations and to prosecute for money laundering (and any other) crimes, is the Public Prosecutor's Office, which may be assisted by the Financial Intelligence Office (*Gabinete de Informação Financeira*).

The GIF is granted the following competency to carry out its duties:

- to receive information provided in accordance with Administrative Regulation no. 7/2006 and to establish and maintain a database with such information;
- to analyse the information received, and report the suspicious money laundering activities to the Public Prosecution Office;
- to provide assistance to law enforcement agencies, judicial authorities and other entities empowered to prevent and prohibit money laundering and terrorist financing crimes, based on their requests with clearly stated reasons, particularly in the form of information giving and technical support;
- to provide for and receive from entities out of Macau SAR information about money laundering and terrorist financing crimes, for the implementation of inter-regional agreements or any other international law instruments;
- to collaborate with public entities to establish and revise anti-money laundering and counter-terrorist financing guidelines they are responsible to issue;
- to develop promotional and educational programmes for public awareness about anti-money laundering counter-terrorist financing; and
- to furnish the Secretary for Security with an annual report on its activities.

1.5 Is there corporate criminal liability or only liability for natural persons?

Companies, even those not regularly incorporated, and associations without legal personality are responsible for the crime of money laundering when committed in their name and in the collective interest: (1) by its bodies or representatives; or (2) by a person under their authority, where the commission of the crime has become possible because of an intentional breach of the duties of supervision or control incumbent on them.

Corporate liability does not exclude individual responsibility of the relevant agents.

The following penalties shall apply to corporations:

- Fine (shall be fixed in days, at least 100 and at most 1,000). Each fine day corresponds to an amount of between MOP 100 and MOP 20,000.
- Judicial dissolution.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

According to Articles 3 and 4 of Law no. 2/2006 (prevention and suppression of the crime of money laundering) and Article 6 of Law no. 3/2006 (prevention and suppression of the crimes of terrorism), as amended by Law no. 3/2017, money laundering and terrorist financing activities are considered as serious criminal offences, punishable with a maximum penalty of 12 years' imprisonment.

1.7 What is the statute of limitations for money laundering crimes?

Under Article 110 of the Macau Criminal Code, the Statute of limitation is 15 years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

This is not applicable in Macau.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The aim of Law no. 6/2016 was to establish a regime to execute decisions to freeze assets under UN Security Council penalty resolutions, adopted in the context of the fight against terrorism and the proliferation of weapons of mass destruction and made applicable to the MSAR by a decision of the People's Republic of China. The scope of application of the law is as follows:

- natural, collective persons and entities in the MSAR or natural persons on board a vessel or aircraft registered in the MSAR;
- residents of the MSAR, regardless of their whereabouts;
- assets in the MSAR owned by a natural, collective person or an entity that is subject to an asset-freezing decision; and
- all transactions or operations related to assets, by any means, directly, totally or partially, in or through the MSAR.

The Chief Executive of the MSAR is competent to execute asset-freezing decisions in the MSAR, with technical assistance from the newly-established Coordinating Commission for the Regime of Freezing of Assets.

In order for assets to be frozen, the act of identification – an act by an international competent institute or a chief executive who identifies a natural, collective person or entity as the subject of an asset-freezing decision – must be published in the Official Gazette. Following publication, it is prohibited to make an asset that is the property or under the control of the identified person or entity available to that party. This section further provides for specific circumstances where:

- co-ownership is involved;
- access to frozen assets is requested;
- administration of frozen assets is required;
- perishable assets are present;
- the process of verification of identification is invoked; and
- liability for damages is excluded.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

To the best of our knowledge, no banks or other regulated financial institutions or their directors, officers or employees have been convicted of money laundering to date.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions are solved by the Macau courts or by the Public Prosecutor's Office, which can decide not to proceed with criminal charges against a subject or a company being investigated. Macau SAR is a Civil Law legal system and under this jurisdiction it is not common to have cases solved in a different manner, i.e. it is not common (and legally acceptable) to have matters related with criminal offences solved by an agreement entered into between the Public Prosecutor and the defendant.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The following administrative authorities may impose anti-money laundering requirements on the respective entities:

- Monetary Authority of Macau and Gaming Inspection and Coordination Bureau (and entities subject to their respective supervision).
- Financial Services Bureau (auditors, accountants and tax advisers).
- Legal Affairs Bureau (public notaries and registrars).
- Macau Trade and Investment Bureau (entities that are under its supervision and which carry out the activities listed in subparagraphs (3), (4) and (6) of paragraph 6) of Article 6 of Law no. 2/2006).
- The Housing Bureau (real estate intermediaries and agents).
- Macau Economic Service (other entities).

Activities with reporting requirements are:

- Buying and selling of real estate.
- Managing of client funds, securities or other assets.
- Managing of bank, savings or securities accounts.
- Organisation of contributions necessary for the creation, operation or management of companies.
- Creation, operation or management of legal persons or entities without legal personality or the buying and selling of enterprises.
- Providers of services, in preparing or performing operations for a customer, within the scope of the following activities:
  1. acting as an agent in forming legal persons;
  2. acting as a director or secretary of a company, a partner or holding of a similar position in relation to other legal persons;

3. providing a registered office, business address, premises, administrative or postal address for a company, or any other legal person or entities without legal personality;
4. acting as a trustee;
5. acting as a partner of a company on behalf of another person; and
6. carrying out the measures necessary for a third party to act in the manner prescribed in subparagraphs (2), (4) and (5).

- Acting as an agent in forming legal persons.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Both the Macau Lawyers Association (lawyers) and the Independent Commission for the Exercise of the Disciplinary Power over Solicitors (solicitors), among other professional associations, impose anti-money laundering requirements, similar to the administrative authorities above, in the following areas:

- Buying and selling of real property.
- Managing of client funds, securities or other assets.
- Managing of bank, savings or securities accounts.
- Organisation of contributions necessary for the creation, operation or management of companies.
- Creation, operation or management of legal persons or entities without legal personality or buying and selling of enterprises.
- Providers of services, in preparing or performing operations for a customer, within the scope of the following activities:
  1. acting as an agent in forming legal persons;
  2. acting as a director or secretary of a company, a partner or holding of a similar position in relation to other legal persons;
  3. providing a registered office, business address, premises, administrative or postal address for a company, or any other legal person or entities without legal personality;
  4. acting as a trustee;
  5. acting as a partner of a company on behalf of another person; and
  6. carrying out the measures necessary for a third party to act in the manner prescribed in subparagraphs (2), (4) and (5).
- Acting as an agent in forming legal persons.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The following government agencies and professional associations are required to carry out supervisory functions and issue instructions/guidelines on anti-money laundering and counter-terrorist financing under Administrative Regulation no. 7/2006:

- The AMCM and Gaming Inspection and Coordination Bureau ("DICJ") (Banks, Insurance and remittance company and money exchangers and Casino operators and gaming promoters).
- The Financial Services Bureau (auditors, accountants and tax advisers).
- The Macau Lawyers' Association (lawyers).
- The Legal Affairs Bureau (public notaries and registrars).
- The Macau Trade and Investment Bureau (entities that are under its supervision and which carry out the activities listed in subparagraphs (3), (4) and (6) of paragraph 6) of Article 6 of Law no. 2/2006).
- The Housing Bureau (real estate intermediaries and agents).
- Macau Economic Service (other entities).

2.4 Are there requirements only at national level?

The requirements are only at the Macau Special Administrative Region's level and not at national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The competent authorities responsible for examination for compliance and enforcement of anti-money laundering requirements are as follows: the Public Prosecutor's Office; the Monetary Authority of Macau (AMCM) and Financial Intelligence Office (GIF); the Monetary Authority of Macau; the Gaming Inspection and Coordination Bureau (entities subject to their respective supervision); the Financial Services Bureau (auditors, accountants and tax advisers); the Macau Lawyers' Association (lawyers); the Independent Commission for the Exercise of the Disciplinary Power over Solicitors (solicitors); the Legal Affairs Bureau (public notaries and registrars); the Macau Trade and Investment Bureau (entities that are under its supervision and which carry out the activities listed in subparagraphs (3), (4) and (6) of paragraph 6) of Article 6 of Law no. 2/2006); the Housing Bureau (real estate intermediaries and agents); and Macau Economic Service (other entities).

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

GIF was established under Executive Ruling no. 227/2006 for the purposes of collecting, analysing and disseminating information on suspicious money laundering and terrorist financing transaction reports, as required by Law no. 2/2006. It is an independent government entity directly under the supervision of the Secretary for Security (previously it was under the supervision of the Secretary for the Economy and Finance).

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There are different types of statute of limitations depending on the type of crime, which may vary from two to 20 years in the serious crimes punishable with imprisonment up to 15 years.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Non-compliance with regulatory requirements shall be deemed as an administrative breach (except in cases of false declarations by the relevant entity). These administrative breaches shall be sanctioned by a fine of between MOP 10,000 and MOP 500,000, or between MOP 100,000 and MOP 5 million depending on whether the offender is a natural or a legal person.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

For individuals, there are no further penalties. For corporations, the court may also decide to force closure of the company convicted of this type of crime.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Besides the administrative proceedings resulting in an administrative penalty (fine), institutions failing to comply with anti-money laundering obligations may be subject to criminal sanctions in case wrongful information is reported to the relevant authorities.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The administrative process is regulated by the rules of the Macau Administrative Code and the criminal process by the Macau Criminal Procedure Code. There are certain rules in both Codes which shall be fulfilled by the respective authorities. Administrative resolutions of penalty actions may or may not be made public. As to the criminal resolutions, they are only made public after there is an accusation by the Public Prosecutor. To our knowledge, there have not been any penalties imposed on financial institutions.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

According to Article 6 of Law no. 2/2006 on prevention and repression of money laundering crimes, the following entities are required to establish control systems for customer due diligence purposes and report suspicious transactions when detected:

- Those subject to the supervision of AMCM.
- Those subject to the supervision of the DICJ, such as entities that operate games of chance, lotteries, mutual bets and promoters of games of chance in casinos.
- Traders of goods of very high unit value, such as entities trading in pawned objects, precious metals, precious stones and luxury transport vehicles, as well as auctioneers.
- Entities engaged in intermediary activities of real estate or in buying real estate for reselling.
- Lawyers, solicitors, notaries, registrars, auditors, accountants and tax advisers, when participating or assisting in the exercise of their professional services, in the operation of:
  - Buying and selling of real property.
  - Managing of client funds, securities or other assets.
  - Managing of bank, savings or securities accounts.
  - Organisation of contributions necessary for the creation, operation or management of companies.
  - Creating, operating or managing of legal persons or entities without legal personality or buying and selling of enterprises.
- Providers of services, in preparing or performing operations for a customer, within the scope of the following activities:
  - Acting as an agent in forming legal persons.
  - Acting as a director or secretary of a company, a partner or holding of a similar position in relation to other legal persons.
  - Providing a registered office, business address, premises, administrative or postal address for a company, or any other legal person or entities without legal personality.
  - Acting as a trustee.
  - Acting as a partner of a company on behalf of another person.
  - Carrying out the measures necessary for a third party to act in the manner prescribed in subparagraphs (2), (4) and (5).

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

As of today, there are no specific laws addressing and regulating cryptocurrency in Macau SAR. Nevertheless, in the last couple of years AMCM has enacted several instructions and warnings related with this matter and according to the regulator point of view "cryptocurrencies are virtual products, but not legal currencies or financial tools. Residents should be aware of fraud and criminal activities associated with cryptocurrencies". In a different guideline, AMCM has also emphasised that any institution providing regulated financial services such as currency exchange, cross-border fund transfer and financial exchange platforms without permission violates relevant provisions of Macau FSA.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Certain institutions, such as banks and other financial institutions, must designate at least one compliance officer responsible for AML/CFT compliance, co-ordination and follow-up of related activities as well as reviewing and determining whether or not to file a suspicious transaction report with the GIF. The AML/CFT Compliance Officer should also coordinate the risk assessment and submit the updated risk assessment report to the AMCM in December of each year. The designation of the AML/CFT Compliance Officer(s) or any subsequent replacement requires prior consent from the AMCM.

In addition to appropriate competence and experience, the following criteria should also be observed:

- the AML/CFT Compliance Officer should have an appropriate management or senior position within the institution's organisational structure;
- the reporting lines should be such that the AML/CFT Compliance Officer's role will not be compromised by undue influence from line management; and
- the AML/CFT Compliance Officer should have timely access to all customer files, transaction records and other relevant information.

Other institutions such as those subject to the supervision of DICJ, (e.g. entities that operate games of chance, lotteries, mutual bets and

promoters of games of chance in casinos) are also required to maintain compliance programmes and to appoint Compliance Officers under the stipulated DICJ Guideline no. 1/2016.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Under Administrative Regulation no. 7/2006, different government agencies and professional bodies are required to issue instructions/guidelines to entities with an obligation to carry out customer due diligence measures and report suspicious transactions.

The reporting entities are required to report suspicious transactions within two working days following the performance of such operations to the GIF. It is stipulated in Article 9 that non-compliance with the duties established in the Administrative Regulation constitutes an administrative offence, which will be punishable with a fine of between MOP 10,000 and MOP 500,000, or MOP 100,000 and MOP 5,000,000, depending on whether the offender is a natural or a legal person.

Suspicious transaction reports can be submitted by mail, addressed to the GIF.

Standard reporting forms should be used when reporting suspicious transactions and such forms can be obtained from the reception counters or downloaded from the websites of relevant supervisory authorities and professional bodies, as well as the GIF.

In addition, "suspicious transaction reports" can also be submitted through encrypted e-mail or online via the STR Reporting System.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Macau regulations refer to occasional transactions as those transactions initiated by customers who do not have a pre-established business relationship with the institutions or initiated by existing customers but not conducted through their accounts, in relation to wire transfers, currency exchanges, encashment of travellers' cheques, money/postal orders, cashier orders, bank drafts, or gift cheques, etc. For all occasional cross-border and domestic wire transfers, regardless of the amount, or any other occasional transactions mentioned above in an amount equal to or exceeding MOP/HKD 120,000 or equivalent in any other currencies, or a few such transactions that appear to be linked (e.g. when several transactions are made by the same customer in a short period of time) and aggregate to an amount equal to or exceeding the aforesaid threshold, proper records of the wire transfer, money change and encashment transactions information should be kept by institutions.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Any natural person who, when entering the Macau Special Administrative Region, carries cash and/or bearer negotiable instruments with a total value equal to or above MOP 120,000, shall declare such value to the Customs Officers.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

In general, Macau financial institutions are required to:

a) Identify, verify and record the identity of customers and the related beneficial owners using reliable and independent source documents, data or information.

b) Understand and obtain information on the nature of the business, ownership and control structure of those legal persons and legal arrangements.

c) Understand and obtain information on the purpose and intended nature of the business relationship.

d) Conduct ongoing due diligence on the business relationship and scrutiny of transactions to ensure consistency with customers' background throughout the course of the relationship.

e) Take particular care in conducting reasonable due diligence measures for the following persons and entities who:

   i) maintain accounts or business relationships, or ask to open accounts or make transactions, but do not appear to act on their own behalf;

   ii) are the beneficiaries of the transactions conducted by professional intermediaries (e.g. lawyers, accountants, etc.) or by any other similar persons or entities;

   iii) are acting on behalf of existing customers and/or connected with any transactions, posing ML/FT or other risks to the institutions; and

   iv) have access to safe deposit boxes not leased by them.

Moreover, there are also account opening procedures and ongoing reviews of customer information in place for banking institutions. In terms of enhanced customer due diligence measures, financial institutions shall exercise special attention in relation to those customers rated as high-risk to safeguard the institution from being used for money laundering or terrorist financing. Institutions should also examine, as far as reasonably possible, the background and purpose of all complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or lawful purpose.

Where the ML/TF risks are higher, institutions should conduct enhanced customer due diligence measures consistent with the risks identified. Enhanced customer due diligence measures that could be applied for higher-risk business relationships include:

i) Obtaining additional information on the customer (e.g. occupation, volume of assets, etc.) by referring to publicly available information, making additional data searches, and/or seeking third-party verification like references from other regulated financial institutions.

ii) Obtaining additional information on the corporate customer, its operation and the individuals behind it.

iii) Updating more regularly the identification documents of the customer and the beneficial owner(s).

iv) Obtaining additional information on the nature of the business relationship.

v) Obtaining additional information on the source of funds and source of wealth of the customer.

vi) Obtaining information on the reasons for intended and/or performed transactions.

vii) Obtaining the approval of senior management to commence or continue the business relationship.

viii) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and by selecting patterns of transactions that need further examination.

ix) Requiring the first payment to be carried out through an account under the customer's name with a bank subject to similar customer due diligence standards.

In addition to the enhanced customer due diligence, institutions shall take other counter measures, e.g., increasing the intensity of monitoring, adoption of specific reporting mechanisms, limiting certain transactions, etc. against those high-risk customers.

All high-risk customers (excluding dormant accounts) shall be subject to more frequent review to ensure that the respective customer due diligence information remains up-to-date and relevant.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Macau Financial Institutions shall not establish or continue business relationships with any shell institutions, in particular shell banks.

3.9 What is the criteria for reporting suspicious activity?

In general, transactions indicating signs of money laundering and/or financing of terrorism crime, or transactions suspiciously involving converting, transferring or dissimulating illegally obtained funds or properties in order to conceal the true ownership and origin of the funds or properties to make them appear to have originated from a legitimate source, are considered suspicious money laundering and/or terrorist financing transactions, or in abbreviation, suspicious transactions.

Institutions should report all suspicious transactions to the GIF within the prescribed time limit, regardless of the amount of the transaction.

Institutions should also make a suspicious transaction report to the GIF when unable to complete transactions (attempted transactions), or customer due diligence, regardless of whether or not the relationship has commenced or the transaction has been conducted.

Institutions should have properly documented procedures with respect to the detection and reporting of the suspicious transactions, which should cover the following:

a) there should be a clearly defined channel for reporting suspicious transactions detected by staff at all levels to the AML/CFT Compliance Officer;

b) the AML/CFT Compliance Officer should maintain, in accordance with the relevant provisions of applicable laws, a register of all such reports submitted by the staff, which should include full details of the suspicious transactions, relevant analysis, reasons for reporting to the GIF or not, follow-up actions and other relevant information; and

c) when the decision is made to report the suspicious transactions detected by the relevant staff, the AML/CFT Compliance Officer is required to report the transactions to the GIF within the prescribed time limit. It is essential that the report of the suspicious transactions should be made swiftly and not be subject to undue delay or bureaucracy.

The report of suspicious transactions should include all relevant information for the identification of the customers specified in AMCM Guidelines and indicate the transactions detected as falling outside the normal pattern of activity of the customers.

Reporting of suspicious transactions should be made in the standard form prescribed by the GIF.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, all companies incorporated in Macau as well as its branches are subject to public registration with the Macau Commercial Registry and this registration includes information about their management. With respect to ownership, the information may not be public but in case of financial institutions subject to a formal authorisation from the local regulator, all relevant information shall be made available to AMCM prior to the issuance of the said authorisation.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Institutions are required to screen payment instructions, in particular those made through wire transfers, in order to ensure that no payments will be made to any persons or entities identified on the sanctions list. Institutions are also required to screen customers and the related parties (including the beneficial owner and any other natural persons having the power to direct the activities of the customer) before establishing a business relationship or conducting occasional transactions exceeding the relevant thresholds.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Bearer shares were eliminated by Law no. 4/2015 and are no longer permitted.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

There are AML/CTF requirements applicable to the gaming industry and its most relevant stakeholders. The requirements are somewhat similar to those in place for financial institutions. Gaming operators are also required to put in place strong compliance teams, report high value and suspicious transactions and appoint an independent compliance Officer and to render significant due diligence over its clients.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

This is not applicable in Macau.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

To the best of our knowledge, there are no additional anti-money laundering measures proposed or under consideration.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The Asia/Pacific Group on Money Laundering (APG), the international organisation on Anti-Money Laundering and Terrorist Financing, published the Mutual Evaluation Report (MER) of Macau SAR, on 1 December 2017. The report has been adopted by all APG members and has undergone a stringent ex-post review process by the global members of the Financial Action Task Force (FATF) to ensure the quality and consistency of the evaluation standard.

According to the mutual evaluation results, among the 11 effectiveness outcomes assessed, Macau SAR obtained six "substantial effectiveness" ratings, which puts the Region among the higher tier of APG members that have been recently evaluated. There were also three "moderate effectiveness" ratings and only two "low effectiveness" ratings. For the technical compliance assessment, which deals with completeness of the legal and institutional framework, out of the 40 FATF Recommendations, Macau SAR has obtained 37 "compliant" and "largely compliant" ratings, and only two "partially compliant" and one "non-compliant" ratings.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Macau was subject to evaluation by the Asia/Pacific Group on Money Laundering (APG), the international organisation on Anti-Money Laundering and Terrorist Financing. The report from such evaluation was made available on 1 December 2017.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The relevant anti-money laundering laws, regulations, administrative decrees and guidance may be obtained from the following Macau SAR websites:

- http://www.gif.gov.mo.
- http://www.amcm.gov.mo.
- http://www.dicj.gov.mo.

Although English is not a Macau SAR official language, most of the materials regarding AML/CTF are available in English.

Pedro Cortés

Rato, Ling, Lei & Cortés – Advogados
Avenida da Amizade 555
Macau Landmark Office Tower, 23rd Floor
Macau

Tel: +853 2856 2322
Email: cortes@lektou.com
URL: www.lektou.com

Pedro Cortés has been a lawyer at Lektou since 2003 and a partner since 2006, having extensive experience in gaming, corporate, finance and IP law.

Pedro is a professional member of the Macau Lawyers' Association, the Portuguese Bar Association, the Brazilian Bar Association (São Paulo), the Hong Kong Institute of Directors, the International Association of Gaming Advisors (IAGA), the International Bar Association (IBA), the Chartered Institute of Arbitrators (CIArb) and the Hong Kong Institute of Arbitrators (HKIA). He is also qualified to work as a lawyer in East Timor and is recognised by the Justice Department of Guangdong as a Cross-border Macau Lawyer. He was lecturer at the Master's programme on Social Sciences – Global Economic Politics, at the Chinese University of Hong Kong and is lecturer of the Law Degree Course of the Portuguese Catholic University (Lisbon School).

Pedro has been a contributor to several legal and non-legal publications, including China Outbound Investments, International Financial Law Review and International Law Office.

Óscar Alberto Madureira

Rato, Ling, Lei & Cortés – Advogados
Avenida da República, nº6
7º Esquerdo
1050-191 Lisboa
Portugal

Tel: +351 213 303 790
Email: madureira@lektou.com
URL: www.lektou.com

Óscar Alberto Madureira is a lawyer at Lektou and is a professional member of the Macau Lawyers' Association, the Portuguese Bar Association and the Hong Kong Institute of Arbitrators (HKIA).

Prior to this, Óscar was a lawyer for Melco Entertainment and for other law offices in Macau. He was also a Legal Consultant for Porto City Hall, for the Portuguese National Traffic and Transportation Department and for the Honorary Consulate of the Republic of Guinea Bissau in Portugal.

Óscar is a member of the Scientifically Counsel of the Rui Cunha Foundation, a lecturer and consultant at CRED-MD – Center for Reflection, Study and Dissemination of Macau SAR Law and an invited lecturer at the University of Saint Joseph, Macau. He is also lecturer of the Law Degree Course of the Portuguese Catholic University (Lisbon School).

Rato, Ling, Lei & Cortés – Advogados (Lektou) is a Macau SAR-based law firm with more than 30 years' experience of legal practice in Macau. Services regularly provided by the firm include issuing legal opinions and advising on Macau Law, helping international companies to start their businesses in Macau and assisting in the reorganisation of economic groups with connections to Macau.

In 2016, Lektou partnered with Zhong Yin Law Firm, in the People's Republic of China, and Fongs, in Hong Kong, to open a new office in Hengqin Island, Zhuhai, PRC – ZLF Law Firm. This is the first law office that unites firms from the two Special Administrative Regions and Mainland China.

In 2017, Lektou opened an office in Lisbon, Portugal, as a part of its internationalisation strategy to position as a legal player in the platform between the PRC and Portuguese-speaking countries.

The academic and professional background, the update and specialisation, together with the experience of the lawyers of Lektou, are the key to answering the increasing demand of the firm's worldwide clients.

Chapter 21

Malaysia

Karen Foong Yee Ling

Raymond Yong

Rahmat Lim & Partners

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the **AMLATFA**) is the primary Malaysian statute dealing with anti-money laundering and anti-terrorism financing. The AMLATFA is federal legislation that has application throughout all states and federal territories of Malaysia.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Offence of money laundering

Section 4 of the AMLATFA stipulates that any person who:

(a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;

(b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;

(c) removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or

(d) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence,

commits a money laundering offence.

Predicate offences

Generally, the terms "proceeds of an unlawful activity" and "instrumentalities of an offence" refer to proceeds or dealings derived or connected with "unlawful activity".

The term "unlawful activity" means:

(a) any activity which constitutes any serious offence or any foreign serious offence; or

(b) an activity which is of such nature, or occurs in such circumstances, that it results in or leads to the commission of any serious offence or any foreign serious offence,

regardless of whether such activity, wholly or partly, takes place within or outside Malaysia.

"Serious offences" mean:

(a) any of the offences specified in the Second Schedule of the AMLATFA;

(b) an attempt to commit any of those offences; or

(c) the abetment of any of those offences.

In addition, the AMLATFA defines "foreign serious offence" as an offence:

(a) against the law of a foreign State stated in a certificate purporting to be issued by or on behalf of the government of that foreign State; and

(b) that consists of or includes an act or activity which, if it had occurred in Malaysia, would have constituted a serious offence.

Tax evasion

Tax evasion constitutes one of the offences under the Second Schedule of the AMLAFTA and is accordingly one of the predicate offences for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes. Under the AMLATFA, any offence under the AMLATFA by, *inter alia*:

(a) any citizen or permanent resident in any place outside and beyond the limits of Malaysia; or

(b) by any person against a citizen of Malaysia; or

(c) by any person who after the commission of the offence is present in Malaysia,

may be dealt with as if it had been committed at any place within Malaysia.

Money laundering of the proceeds of foreign crimes is punishable. Please refer to the definition of foreign serious offences in question 1.2 above.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Depending on the nature of the crime, the investigation of offences under the AMLATFA may be conducted by various enforcement agencies including the Royal Malaysia Police or the competent authority appointed pursuant to the AMLATFA to implement the provisions of the AMLATFA, the Central Bank of Malaysia, Bank Negara Malaysia (**BNM**). As the financial services regulator, BNM

is empowered to investigate money laundering cases relating to the laws administered by BNM such as the Financial Services Act 2013 and the Islamic Financial Services Act 2013.

No prosecution for an offence under the AMLATFA may be instituted except with the written consent of the Attorney General of Malaysia in his capacity as Public Prosecutor.

1.5 Is there corporate criminal liability or only liability for natural persons?

Criminal liability in respect of offences under the AMLATFA extends to both corporates and natural persons. By virtue of Section 2 and 3 of the Interpretation Acts 1948 and 1967, the term "person" under the AMLATFA includes a body of persons, corporate or unincorporate.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Different offences under the AMLATFA have different maximum penalties. The maximum penalty for a money laundering offence under Section 4 of the AMLATFA is imprisonment for 15 years and a fine of not less than five times the sum or value of the proceeds of the unlawful activity or instrumentalities of the offence at the time the offence was committed or RM5 million, whichever is the higher.

1.7 What is the statute of limitations for money laundering crimes?

There is no statutory time limit for prosecution of money laundering offences under the AMLATFA.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

There are no parallel state or provincial criminal offences for money laundering. Enforcement is only at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

There is no separate forfeiture or confiscation regime apart from that set out under the AMLATFA in relation to money laundering offences.

In any prosecution for a money laundering offence under Section 4 of the AMLATFA or a terrorism financing offence, the court will make an order for the forfeiture of any property which is proved to be:

(a) the subject matter or evidence relating to the commission of such offence;

(b) terrorist property;

(c) the proceeds of an unlawful activity; or

(d) the instrumentalities of an offence,

where:

(i) the offence is proved against the accused; or

(ii) the offence is not proved against the accused but the court is satisfied that:

(ia) the accused is not the true and lawful owner of such property; and

(ib) no other person is entitled to the property as a purchaser in good faith for valuable consideration.

Where in respect of any property seized under the AMLATFA, there is no prosecution or conviction under Section 4 or a terrorism financing offence, the Public Prosecutor may, before the expiration of 12 months from the date of the seizure, or where there is a freezing order, 12 months from the date of the freezing, apply to a judge of the High Court for an order of forfeiture of that property if he is satisfied that such property is:

(a) the subject matter or evidence relating to the commission of such offence;

(b) terrorist property;

(c) the proceeds of an unlawful activity; or

(d) the instrumentalities of an offence.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

We have not identified any cases in which financial institutions or their directors, officers or employees have been convicted of money laundering under the AMLATFA, although we are aware that charges have been brought against former bank employees for money laundering.

In 2015, BNM imposed an administrative fine of RM53.7 million on AMMB Holdings Bhd (Ambank Group). Whilst the exact reasons for the fine have not been disclosed, it was announced that the fine had been imposed as a result of non-compliance with anti-money laundering and counter-terrorism financing obligations under the Financial Services Act 2013 and the Islamic Financial Services Act 2013.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions are resolved through the judicial process. Malaysian judgments are publicly available online.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The principal anti-money laundering requirements are contained in the AMLATFA. The AMLATFA makes it an offence for any person to engage in or abet the commission of money laundering and terrorist financing, and seeks among other things, to implement measures for the prevention of money laundering and terrorism financing offences. These measures include the imposition of obligations on reporting institutions (as described in the First Schedule of the AMLATFA) for reporting of transactions exceeding a specified threshold, and suspicious transactions, as well as customer due diligence.

The reporting institutions under the AMLATFA include, *inter alia*, banks and insurers as well as professionals such as advocates and solicitors.

BNM as the competent authority appointed under the AMLATFA is empowered to issue to reporting institutions guidelines, circular or notices to give full effect to or for carrying out the provisions of the AMLATFA. In this regard, BNM has issued various guidelines to reporting institutions based on the industry sector including, *inter alia*:

(a) banking and deposit-taking institutions;

(b) insurance and takaful;

(c) money services business;

(d) electronic money and non-bank affiliated charge & credit card;

(e) designated non-financial businesses and professions (**DNFBPs**) and other non-financial sectors; and

(f) digital currencies.

Additionally, the Labuan Financial Services Authority has sectoral guidelines applicable to Labuan entities relating to sectors such as banking, insurance and takaful, trust company and capital market and other business sectors. The Securities Commission has issued guidelines on prevention of money laundering and terrorism financing for capital market intermediaries under its purview.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes, there are anti-money laundering requirements imposed by self-regulatory organisations and professional associations, including the Bar Council of Malaysia (advocates and solicitors practising in West Malaysia) and the Malaysia Institute of Accountants (professional accountants).

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Failure to comply with the circulars or guidelines issued by the relevant self-regulatory organisations or professional associations may result in disciplinary actions against the members.

2.4 Are there requirements only at national level?

These requirements are only applicable at the national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

BNM as the competent authority as well as the relevant supervisory authority of a reporting institution are responsible for examination for compliance and enforcement of anti-money laundering requirements. Under Section 21 of the AMLATFA, the relevant supervisory authority of a reporting institution may, *inter alia*, examine and supervise reporting institutions, and regulate and verify, through regular examinations, that a reporting institution adopts and implements compliance programmes to guard against and detect any offence under the AMLAFTA. The policy documents and guidelines issued by BNM and supervisory authorities such as the Labuan Financial Services Authority and the Securities Commission are publicly available on their websites. Please refer to question 2.1 above.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the Financial Intelligence Unit (**FIU**), established within the Financial Intelligence and Enforcement Department in BNM manages and provides comprehensive analysis of the financial intelligence received relating to money laundering and terrorism financing.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statutory time limit for competent authorities to bring enforcement actions.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Under Section 22 of the AMLATFA, the maximum penalty for failure by a reporting institution to ensure the reporting institution's compliance with its obligations under Part IV (Reporting Obligations) of the AMLATFA is a fine not exceeding one million ringgit or imprisonment for a term not exceeding three years or both. In the case of a continuing offence, there will be an additional fine not exceeding three thousand ringgit for each day or part thereof during which the offence continues to be committed.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

In minor cases of non-compliance, BNM or the relevant supervisory authority may issue a warning letter to the relevant reporting institution.

Under the AMLATFA, BNM may upon application to the court and satisfying the court that a reporting institution has failed without reasonable excuse to comply with any obligations under the AMLATFA, obtain an order against the officers or employees of that reporting institution on such terms as the court deems necessary to enforce compliance with such obligations. Notwithstanding this, BNM may also direct or enter into an agreement with any reporting institution to implement any action plan to ensure compliance with its obligations under Part IV (Reporting Obligations) of the AMLATFA.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Yes, violations of anti-money laundering obligations are also subject to criminal sanctions including imprisonment and fines.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process for assessment and collection of sanctions is dependent on the relevant competent authority or enforcement agency. Details of sanctions imposed are not always made publicly available – these could include, for example, supervisory letters, reprimand/warning and administrative fines or penalties. Generally, administrative decisions or sanctions may be challenged by way of judicial review of the High Court. However, this option is rarely pursued in practice.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Reporting institutions under the AMLATFA are subject to anti-money laundering requirements including record-keeping, customer due diligence and reporting of suspicious transactions. The full list of reporting institutions can be found in the First Schedule of the AMLATFA.

These include, *inter alia*:

(a) activities carried out by a licensed bank, licensed investment bank, licensed insurer, approved financial adviser, approved insurance broker, approved issuer of designated payment instrument and approved money broker under the Financial Services Act 2013;

(b) activities carried out by a holder of a licence under the Capital Markets and Services Act 2007;

(c) activities carried out by an advocate and solicitor as defined in the Legal Profession Act 1967; and

(d) activities carried out by a member as defined in the Accountants Act 1967.

Please refer to question 2.1 above for a brief description of the obligations imposed on reporting institutions.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Under the First Schedule to the AMLATFA, a reporting institution includes any person who provides any or any combination of the following services:

(a) exchanging digital currency for money;

(b) exchanging money for digital currency; and/or

(c) exchanging one digital currency for another digital currency,

whether in the course of carrying on a digital currency exchange business or otherwise.

BNM has issued the Anti-Money Laundering and Counter Financing of Terrorism (**AML/CFT**) – Digital Currencies (Sector 6) policy document which is applicable to such reporting institutions. Apart from the usual reporting obligations applicable to all reporting institutions relating to, for example, customer due diligence and recordkeeping, sector 6 reporting institutions must declare their details to BNM in the form specified under the Sector 6 policy document.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes, under Section 19 of the AMLATFA, a reporting institution is required to adopt, develop and implement internal programmes, policies, procedures and controls to guard against and detect any offence under the AMLAFTA. The programmes must include the establishment of procedures to ensure high standards of integrity of its employees and a system to evaluate the personal, employment and financial history of employees, ongoing employee training programmes to instruct employees with regard to their responsibilities specified under the AMLATFA, the appointment of compliance officers, and an independent audit function to check for compliance with such programmes.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

A reporting institution must maintain any account, record, business correspondence and document relating to an account, business relationship, transaction or activity with a customer or any person as well as the results of any analysis undertaken, as the case may be, for a period of at least six years from the date the account is closed or the business relationship, transaction or activity is completed or terminated.

A reporting institution must keep a record of any transaction involving the domestic currency or any foreign currency exceeding such amount as BNM may specify, and must report to BNM any transaction exceeding such amount as BNM may specify.

Under a circular issued by BNM on 28 December 2018, the relevant threshold for making a cash threshold report (**CTR**) is RM25,000 and above in a day. CTR obligations are imposed on banking institutions and licensed casinos. Such reporting institutions are required to submit a CTR to BNM in respect of any cash transaction exceeding RM25,000 and above in a day. This includes cash transactions involving physical currencies (domestic or foreign currency) and bearer negotiable instruments such as travellers' cheques but bank drafts, cheques, electronic transfers or fixed deposit rollovers or renewals are excluded. The requirements for making a CTR are applicable to single or multiple cash transactions within the relevant amount specified in a day, and where there are deposit and withdrawal transactions, the amounts must be aggregated and not offset against each other.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Apart from large cash transactions, reporting institutions must also file a Suspicious Transaction Report with the Financial Intelligence and Enforcement Department of BNM in respect of any transaction (attempted or proposed), regardless of the amount, where such transaction meets the criteria specified in question 3.9 below.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Travellers entering or leaving Malaysia with cash and/or negotiable bearer instruments (e.g. travellers' cheques, bearer cheques) exceeding an amount equivalent to USD10,000 must make a declaration.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Under the Sector 1 guidelines issued by BNM applicable to licensed banks, the customer due diligence ("**CDD**") requirements to be undertaken by reporting institutions include:

(a) identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;

(b) identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and

(c) understanding, and, where relevant, obtaining information on, the purpose and intended nature of the business relationship.

Specific CDD measures are set out in the Guidelines in relation to documents and information to be obtained in relation to, for example, an individual customer and beneficial owner, legal persons, legal arrangements, and clubs, societies and charities.

Enhanced CDD is required to be performed where the money laundering/terrorism financing risk is assessed as higher risk, for example, upon determination that a customer or a beneficial owner is a foreign politically exposed person.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes, under the Sector 1 guidelines issued by BNM applicable to licensed banks, reporting institutions must not establish or have any business relationship with shell banks.

3.9 What is the criteria for reporting suspicious activity?

A reporting institution must promptly report to BNM:

(a) any transaction where the identity of the person involved, the transaction itself or any other circumstances concerning that transaction gives any officer or employee of the reporting institution reasons to suspect that the transaction involves proceeds of an unlawful activity or instrumentalities of an offence; or

(b) any transaction or property where any officer or employee of the reporting institution has reason to suspect that the transaction or property involved is related or linked to, is used or is intended to be used for or by, any terrorist act, terrorist, terrorist group, terrorist entity or person who finances terrorism.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes. The Companies Commission of Malaysia (**CCM**) maintains a public registry of companies, businesses and Limited Liability Partnerships (**LLP**). Reports containing information such as a company's profile, particulars of directors/officers, particulars of share capital, particulars of shareholder and company charges are publicly available online for purchase.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, under the Sector 1 guidelines issued by BNM applicable to licensed banks, accurate originator information pertaining to name, account number (or unique reference number if there is no account number) which permits traceability of the transaction, and address (or *in lieu* of address, date and place of birth) and beneficiary information pertaining to name and account number (or unique reference number if there is no account number) which permits traceability of the transaction, are required. This applies to reporting institutions which are ordering institutions for message or payment instructions for all cross-border wire transfers involving an amount equivalent to RM3,000 and above. Insofar as domestic wire transfers are concerned, the information accompanying the wire transfer should include the originator information as indicated for cross-border wire transfers (unless the information can be made available to the beneficiary institution and relevant authorities by other means).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No. Under the Companies Act 2016, a company is prohibited from issuing bearer shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes. BNM has issued the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Designated Non-Financial Businesses and Professions (**DNFBPs**) and Other Non-Financial Sectors (Sector 5) policy document to address the requirements for non-financial institution businesses. There are specific CDD requirements to be complied with by a licensed casino, licensed gaming outlet, dealer in precious metals and stones and moneylender as attached in Annexures I–V of the Sector 5 policy document.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

BNM has issued policy documents pertaining to various business sectors. Please see response to question 2.1 above for the full list of the policy documents.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

We are not aware of any material reforms being proposed at this stage.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

A Mutual Evaluation Report dated September 2015 by the FATF is accessible here: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Malaysia-2015.pdf, and the 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating by the FATF dated October 2018 is accessible here: http://www.fatf-gafi.org/media/fatf/documents/reports/fur/FUR-Malaysia-2018.pdf.

Under the 2018 Report and in light of Malaysia's progress since the Mutual Evaluation Report was adopted, Malaysia's technical compliance with the FATF Recommendations has been re-rated and Malaysia is generally rated as "partially compliant", "compliant" and "largely compliant" in respect of the 40 FATF Recommendations. The FATF has continued to place Malaysia in "enhanced follow-up" on the basis that it had a moderate level of effectiveness for seven of the 11 effectiveness outcomes (FATF Procedures, para. 79(a)(iii)). According to the enhanced follow-up process, Malaysia will continue to report back to the FATF on progress to strengthen its implementation of AML/CFT measures.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes, please see response to question 4.2 above.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Yes, the materials are available in English.

The AMLATFA, sectoral policy documents issued by BNM and other circulars, guidance and technical notes can be accessed at BNM's AML/CFT website: http://amlcft.bnm.gov.my/AMLCF T07.html.

Karen Foong Yee Ling

Rahmat Lim & Partners
Suite 33.01 Level 33
The Gardens North Tower
Mid Valley City, Lingkaran Syed Putra
59200 Kuala Lumpur
Malaysia

Tel: +603 2299 3903
Email: karen.foong@rahmatlim.com
URL: www.rahmatlim.com

Karen is a Principal in Rahmat Lim & Partners' Regulatory & Compliance Department.

Karen has experience in advising financial institutions and corporations on financial services laws and regulations. These include advising on licensing, regulatory, compliance and other conduct of business requirements for banking, securities, derivatives, asset management and other capital markets businesses.

She has also assisted domestic and foreign entities in relation to regulatory enquiries and investigations in connection with potential, alleged or actual breaches of laws or binding guidelines.

Karen graduated from the University of Reading with an LL.B. Law degree in 2008 and the University of Oxford with the Bachelor of Civil Law in 2011. She was admitted as an Advocate & Solicitor of the High Court of Malaya in 2010.

Raymond Yong

Rahmat Lim & Partners
Suite 33.01 Level 33
The Gardens North Tower
Mid Valley City, Lingkaran Syed Putra
59200 Kuala Lumpur
Malaysia

Tel: +603 2299 3810
Email: raymond.yong@rahmatlim.com
URL: www.rahmatlim.com

Raymond heads the Regulatory & Compliance Department in Rahmat Lim & Partners.

Raymond regularly deals with the Malaysia Competition Commission ("MyCC") and represents clients in investigations, the lodgement of complaints, and leniency applications. He has appeared before the Competition Appeal Tribunal in an appeal against a finding by the MyCC of an abuse of a dominant position and also represented a trade association on its exemption application to the MyCC.

He also advises clients on compliance with the Personal Data Protection Act 2010, and has led several projects that involve exploring and charting business processes of clients.

Raymond advises financial institutions, in particular banks, payment system operators and payment instrument issuers, on the licensing and regulatory aspects of their businesses.

He is recognised as a Leading Individual in Competition and Antitrust by *The Legal 500 Asia Pacific* and by *Chambers Asia-Pacific* which noted his "very sound knowledge". Clients appreciate his provision of "easy-to-understand and practical" information. He is also recommended by *The Global Competition Review* for competition work.

Raymond graduated with a Bachelor of Commerce and an LL.B. degree from The University of Melbourne, Australia.

RAHMAT LIM & PARTNERS
IN ASSOCIATION WITH ALLEN & GLEDHILL (SINGAPORE)

Established in 2010 with slightly more than a dozen lawyers, Rahmat Lim & Partners has grown to become one of the largest corporate law firms in Malaysia. With over 90 lawyers in Kuala Lumpur, and as part of the Allen & Gledhill network, we handle a wide range of domestic and cross-border matters, including some of the most significant and complex transactions involving Malaysia. Our distinctive culture reflects the DNA which runs deep within the A&G network, as highlighted by our use of the same market-leading best practices and cutting-edge legal technology.

Representing a broad range of clients including the leading corporates of the region, our clients are at the heart of our practice. In less than a decade, Rahmat Lim & Partners has achieved top-tier rankings by notable legal directories and publications in major practice areas, and regularly receives accolades and recognition from industry watchers.

Malta

Dr. Emma Grech

Dr. Christina Laudi

City Legal

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Anti-money laundering and the combatting of financial terrorism ('AML/CFT') are principally regulated by the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta) ('PMLA') and its subsidiary legislation, the Prevention of Money Laundering and Funding of Terrorism Regulations (Subsidiary Legislation 373.01 of the Laws of Malta) ('PMLFTR'), which have effectively transposed the Fourth AML Directive (Directive (EU) 2015/849 ('4AMLD')) into Maltese law.

The investigation and prosecution of money laundering and the funding of terrorism ('ML/FT') are regulated by Article 3 PMLA whereby every person charged with an offence shall be tried in the Criminal Court or before the Court of Magistrates as a court of criminal judicature in Malta or Gozo and as directed by the Attorney General ('AG'). As elaborated upon in question 1.4 hereunder, the Financial Intelligence Analysis Unit ('FIAU') does not prosecute ML/FT, but aids in the process of prosecution as a result of its supervisory nature.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

For prosecution to succeed, there must be the conversion or transfer of property with the knowledge or suspicion that such property is derived, whether directly or indirectly, from criminal activity, and this for the purpose of concealing or disguising the origin of the property or assisting those involved in criminal activity. The same applies to the proceeds of said property. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property with the knowledge or suspicion that such property is derived, directly or indirectly, from criminal activity or from an act of participation in criminal activity also constitute ML. Further to this, the acquisition, possession and use of said property and the retention of said property without a reasonable excuse is likewise an offence. Any attempts at these actions as per Article 41 of the Criminal Code (Chapter 9 of the Laws of Malta) ('CC'), or complicity in terms of Article 42 CC are also defined as ML.

Whereas the underlying criminal activity (predicate offence) from which funds originate is an essential element for prosecution, Article 2(2) PMLA specifically states that a person may still be convicted of ML in the absence of a judicial finding of guilt in respect of the underlying criminal activity. Its existence may be established through circumstantial or other evidence without it being necessary for the prosecution to prove or specifically pinpoint the criminal activity. A person can be accused of ML even though the predicate offence has not been established, as long as it can be proved beyond reasonable doubt that the source of such money or property was derived from criminal activity. The offender may be charged separately for the predicate offence.

As of 31 May 2005, and via Legal Notice 176 of 2005, Malta no longer has a restricted list of predicate offences. All criminal offences are predicate offences. Tipping-off is also an offence. As a defence, the accused must prove that he did not know or did not suspect that the disclosure was likely to prejudice the investigation. Tax evasion and all related tax crimes are also deemed to be predicate offences.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Article 9 PMLA refers to situations which involve proceeds found outside of Malta, and the powers of investigation by Maltese authorities in connection with offences cognisable by courts outside of Malta. Article 10 PMLA deals with an extraterritorial request to the AG for the temporary seizure of all or any of the moneys or property, movable or immovable or a person charged or accused in proceedings before extraterritorial courts. Conflicts arise in scenarios where the predicate offence is or is not a crime in that relative jurisdiction.

The FIAU also features in the context of cross-border cases. It cooperates with similar foreign, national and supranational bodies, authorities and, or agencies in coordinating and exchanging information and in imposing administrative penalties and, or implementing other measures.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The FIAU is the government agency established under the PMLA responsible for collecting, processing, analysing and disseminating information within the scope of preventing ML/FT and ensuring

compliance with the relevant laws and regulations. Upon receiving a report or tracking irregular activity, it must forward said report to the Commissioner of Police.

The investigative process is led by the Economic Crimes Unit within the Malta Police Force, more specifically the Money Laundering Unit. It secures evidence and witnesses both internationally and nationally. It is the police who proceed to prosecute in court in conjunction with the AG's office. The AG directs how a person is to be charged with the relative offence and this after taking into consideration various factors, including the person's age and the value of the property allegedly laundered.

1.5 Is there corporate criminal liability or only liability for natural persons?

Yes, corporate liability is included. Article 3(2) PMLA states that when an offence is committed by a body or persons, whether corporate or unincorporate, every person who at the time of the commission of the offence had an executive or administrative role shall be guilty of an offence unless he proves that the offence was committed without that person's knowledge and that he exercised all due diligence to prevent the commission of the crime. Article 3(4) PMLA specifically vests legal representation in the alleged offender, and where said legal representation no longer vests in that person, it shall lie with the replacing persons in his/her stead or other referred persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Article 3(1) PMLA establishes that the maximum punishment is a fine not exceeding €2,500,000 or imprisonment for a period not exceeding 18 years or both. As for legal entities, there are three punishments: that given to the actual individual within the corporate body; the penalty given to the corporate body; and the subsequent forfeiture of proceeds of the corporate body by the Government.

Furthermore, non-compliance with the ML/FT procedures under the PMLFTR is punishable with administrative sanctions reaching a maximum of a €50,000 fine and/or two years' imprisonment.

1.7 What is the statute of limitations for money laundering crimes?

As the PMLA establishes a maximum penalty of 18 years' imprisonment for ML offences, the CC states that crimes liable to imprisonment for a term of not less than 20 years are barred by a lapse of 15 years. Whereas the PMLFTR awards two years' imprisonment, these crimes are then barred by a lapse of five years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Enforcement is at a national level as Malta is an island and has no provinces/states.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The PMLA provides for the confiscation of property. In addition to Article 23 CC, i.e. the forfeiture of the *corpus delicti* (evidence of the crime), the court shall order the forfeiture in favour of the Government of the proceeds or of such property the value of which corresponds to the value of such proceeds (any economic advantage) and any property in the possession or under the control of any person found guilty and deemed to be derived from the offence of ML. The definition of 'property' includes movables or immovables, in or outside of Malta.

Article 4 of the Confiscation Orders (Execution in the European Union) Regulations (Subsidiary Legislation 9.15 of the Laws of Malta) states that the AG is competent to receive confiscation orders issued in the issuing State and to transmit to the executing State his own confiscation orders as issued in Malta by a court of criminal jurisdiction. When the AG receives a request by a judicial authority to be enforced in Malta made by a foreign court, an action is brought. Following legal procedures and a hearing, if enforcement of the order is obtained, then the property is confiscated by the Government. The AG may issue the precautionary acts needed. Confiscation can be an additional punishment to a fine and/or imprisonment, or it can occur via an order made by Malta or to Malta and subsequently enforced through a judgment given by the civil courts. The latter can occur without a criminal conviction and has more of a precautionary nature.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

No convictions against said institutions and individuals exist.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions are resolved through the courts. There are instances where a lesser sentence of imprisonment is given in return for a larger fine. In addition, the FIAU imposes administrative sanctions which are public. In 2018 two penalties were given, one of €38,750 and the other of €15,000.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The FIAU is responsible for imposing AML/CFT requirements on all 'subject persons' and is regulated under Part II PMLA. It has published the sector-specific Implementing Procedures Part I and Part II ('IPI/IPII') which must be adhered to by subject persons. The IPI/IPII comprise an interpretive tool for the PMLA/PMLFTR while simultaneously assisting subject persons in designing systems for the prevention and detection of ML/FT. Measures to be taken include customer due diligence ('CDD'), mandatory risk procedures and the use of a risk-based approach, diligent recordkeeping and reporting procedures, and the provision of training to employees. For further information, please refer to question 3.1.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Reference is made to supervisory authorities which are deemed to be agents of the FIAU. The FIAU upon request or its own motion shall cooperate and exchange information with a supervisory authority when this would assist in AML/CFT. The Malta Financial Services Authority ('MFSA') conducts supervision amongst financial services licence holders and the Malta Gaming Authority does the same amongst licensed gaming operators. The subject person is nonetheless always responsible for providing the information requested.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Supervisory bodies are limitedly responsible for compliance and enforcement as they monitor their members passing on information to the FIAU which then takes enforcement action.

2.4 Are there requirements only at national level?

The requirements are only at a national level as Malta is an island and has no states/provinces. These comprise, predominantly, the PMLA, the PMLFTR, the National Coordinating Committee on Combating ML/FT Regulations (Subsidiary Legislation 373.02 of the Laws of Malta) as well as the IPI/IPII.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Supervisory bodies aid the FIAU with compliance and monitoring in specific areas and professions. The FIAU then enforces, whilst overall retaining its compliance and monitoring obligations. All of the criteria that would lead to investigations are available on the FIAU website (http://www.fiumalta.org/).

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The FIAU is Malta's designated government FIU agency.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Please refer to question 1.7 for the applicable statute of limitations.

For details regarding the FIAU, please refer to the information contained in the above questions.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The FIAU can in these cases act without the need for a court hearing and judgment. Under the PMLFTR, administrative failures are:

- Non-compliance with procedures to prevent ML/FT such as:
  - failing to maintain/apply procedures for CDD, recordkeeping and reporting; and
  - failing to establish internal control, risk assessment, risk management, compliance management and communications;
- commission of an offence under the PMLFTR by corporate/unincorporated bodies and other associations of persons;
- false declaration/false representation by an applicant for business;
- failure to carry out CDD;
- failure to carry out reporting procedures and obligations;
- tipping-off; and
- non-compliance with the IP, guidance, directives issued by the FIAU in terms of the PMLA and PMLFTR.

Administrative penalties may not exceed €50,000. There are a number of fines awarded in addition to imprisonment under the PMLA and these do not exceed €11,646.87.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The PMLFTR provides for reprimands in writing. It can also give one-time fixed penalties and, or penalties on a daily cumulative basis. The minimum daily penalty levied is of €250.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Apart from the PMLA, the PMLFTR provide for criminal sanctions such as:

- non-compliance with procedures (Regulation 4(5));
- a false declaration/false representation by an applicant for business (Regulation 7(10)); and
- tipping off (Regulation 16(1)).

All of these are subject to a fine not exceeding €50,000, or to imprisonment for a term not exceeding two years or both. A disqualification order can also be imposed on company officials for a specified period set by the courts which may be a minimum of one year and a maximum of 15 years.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

When a sanction is imposed by the FIAU under the PMLFTR, the subject person is informed of the potential breach detected and the possibility of an administrative sanction. Representations by the person are requested following which an internal evaluation is made by the Compliance Monitoring Committee. Should fault be found, reasons shall be given. Said sanction must be paid within 14 days. Instead of sanctions, warnings in writing may also be issued as well as in the course of its compliance/monitoring function. If a person feels aggrieved and the sanction exceeds €5,000, an appeal may be lodged both on points of fact and law. The appeal shall lie to the Court of Appeal (Inferior Jurisdiction) and the proceedings shall be

heard *in camera*, following which the judgment shall not be published. Administrative penalties imposed and not appealed are recoverable as a civil debt. Administrative penalties imposed which exceed €10,000 and which have become final and due shall be subject to publication according to the policies and procedures established by the Board of Governors of the FIAU.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

As mentioned further above, AML/CFT requirements are applicable to 'subject persons', which are defined in Regulation 2 PMLFTR as, 'any legal or natural person carrying out either relevant financial business or relevant activity'.

'Relevant activity' includes, when acting in the exercise of their professional activities: auditors; external accountants; tax advisors; real estate agents; in the context of particular transactions, such as when they assist clients with the opening of bank accounts or the creation of companies, independent legal professionals, including lawyers; fiduciary and company services providers; licensed gaming operators; and, where the transaction in question involves payment in cash of €10,000 or more, persons engaged in the trading of goods.

In turn, 'relevant financial business' covers: activities carried out by the credit institutions; payment institutions and electronic money institutions; insurance undertakings and intermediaries; recognised, licensed or notified collective investment schemes and fund administrators; services providers licensed under the Investment Services Act (Chapter 370 of the Laws of Malta); services providers licensed under the Retirement Pensions Act (Chapter 514 of the Laws of Malta); safe custody services providers; regulated markets and the Central Securities Depository; VFA agents and licence holders within the meaning of the Virtual Financial Assets Act (Chapter 590 of the Laws of Malta) ('VFAA') and issuers of virtual financial assets; and any other associated activity. Any of the above relevant financial business activities carried out by branches established in Malta will also be subject to AML/CFT requirements.

The requirements, as principally deriving from the PMLA/PMLFTR, IPI/IPII, render it incumbent upon subject persons – including financial institutions – to implement robust AML/CFT systems and policies and procedures, including recordkeeping, reporting processes and internal controls. Subject persons are compelled to provide information to the relevant authorities on request. In addition, and as of March 2019, a subject person is required to submit a sector-specific annual Risk Evaluation Questionnaire to the FIAU regarding its set-up, risk assessment, and preventative measures.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

AML/CFT requirements are to be likewise applied to VFA agents, licence holders under the VFAA and issuers of virtual financial assets. These entities will also be expected abide by any IPII and, or sector-specific guidance that may be issued from time to time.

Notably, local AML/CFT requirements applicable to the VFA sector go beyond the scope of the Fifth AML Directive (Directive (EU) 2018/843), which is to take effect by 10 January 2020. Whereas Maltese legislation imposes AML/CFT obligations on all VFA service providers, the former regime only applies to cryptocurrency exchanges and custodian wallet providers.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes. Regulation 5(5) PMLFTR imposes the requirement on subject persons – including financial institutions – to, in a manner that is appropriate to the size and nature of the business, have effective AML/CFT systems and policies and procedures, as well as internal controls, in place. Subject persons are required to implement compliance management processes, employee screening policies and training programmes, as well as adopt sufficient reporting mechanisms. Where proportionate, an independent audit function should be set up to test these internal controls.

In addition, subject persons must appoint a Money Laundering Reporting Officer ('MLRO') which will assist in the coordination of its AML/CFT framework. The MLRO will be responsible for the oversight of the subject person's AML/CFT compliance.

Businesses are required to detail their compliance programmes in an internal AML/CFT procedures manual.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There are no fixed 'thresholds' *vis-à-vis* large transactions. Subject persons faced with sizable transactions are bound to comply with general AML/CFT recordkeeping and reporting requirements as set out, predominantly, in Regulations 13 and 15 PMLFTR. That said, however, section 3.1.5.1 IPI stipulates that subject persons are to pay special attention to 'complex or large transactions', which, 'have no apparent economic or visible lawful purpose', establishing their findings in writing. The findings should not automatically be reported to the FIAU or the relevant supervisory authority, but instead made available on request.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, there are currently no routine-based reporting requirements.

The obligation to report arises in the context of suspicious activity. Such reporting is to be carried out with due regard to the requirement in Regulation 15(3) PMLFTR. This states that, where a subject person knows, suspects or has reasonable grounds to suspect that funds are the proceeds of crime or are related to FT, or that a person may have been, is, or may be connected with ML/FT, that subject person is to report the same to the FIAU via a Suspicious Transaction Report ('STR'). An STR is to be made as soon as is reasonably practicable, but no later than five working days from when the knowledge or suspicion first arose. STRs should be submitted to the FIAU in accordance with the guidance provided on the FIAU website.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There are no specific reporting requirements regarding cross-border transactions. Subject persons are however required to inform the FIAU of any business relationships or transactions with persons from 'non-reputable jurisdictions' – as defined in Regulation 2 PMLFTR – which, in effect, do not apply measures equivalent to those laid down in the PMLFTR. The FIAU may, in collaboration with the relevant supervisory authority, discontinue any such business relationships, or prohibit the relevant transactions from being carried out.

Reference must also be made to the obligation to submit STRs as outlined in question 3.5 above.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Subject persons – including financial institutions – are to establish due diligence procedures for identifying and verifying the identity of a prospective customer. A customer may be a legal or natural person who: (i) seeks to form, or has formed, a business relationship with a subject person; or (ii) seeks to carry out an occasional transaction with a subject person.

CDD measures shall, however, only be applied in the context of occasional transactions when these involve: (i) a transaction of €15,000 or more; (ii) a money transfer or remittance within the meaning of the EU Funds Transfer Regulation (Regulation (EU) 2015/847) (the 'Funds Transfer Regulation') amounting to €1,000 or more; and (iii) a transaction of €2,000 or more in the context of licensed gaming operators. The incorporation of companies and, or the provision of tax advice by subject persons shall also be considered to constitute 'occasional transactions', thereby necessitating CDD.

In the context of business relationships, and following the verification of a prospective customer's details, which verification is carried out by the subject person by – as the case may be – viewing official documentation issued by independent sources, such as a government authority, the subject person will need to obtain details on the purpose and intended nature of said relationship. The information the subject person may need to collect in these circumstances includes: data of the customer's business or employment; the source and origin of funds the customer will be using in the business relationship; and the expected level and nature of the activity to be undertaken through the relationship. This information must be kept up-to-date, thereby enabling a business to amend its customer risk assessment if circumstances change, and, if necessary, carry out further CDD.

In higher-risk situations, subject persons must apply enhanced due diligence, namely: (i) where the customer has not been physically present for identification purposes; (ii) when transacting with politically exposed persons, or 'PEPs', such as Heads of State and Members of Parliament; (iii) in a cross-border correspondent banking relationship scenario; (iv) where the business relationship or a transaction is connected to a 'high-risk' jurisdiction (as acknowledged by the EU); and, generally (v) any situation where there may be a greater risk of ML/FT. Enhanced due diligence may necessitate: (i) obtaining additional information to establish the customer's identity; (ii) applying supplementary measures to check the documentation supplied; and (iii) taking adequate steps to establish the source of wealth and funds involved.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

In terms of Regulation 11(4) PMLFTR, subject persons carrying out relevant financial business are prohibited from entering or continuing correspondent relationships with shell institutions. Moreover, they are required to take appropriate measures to ensure that they do not enter into or continue correspondent relationships with respondent institutions which are known to permit their accounts to be used by shell institutions.

Regulation 2 PMLFTR defines a 'shell institution' as an institution carrying out activities equivalent to relevant financial business, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is not affiliated with a regulated financial group.

3.9 What is the criteria for reporting suspicious activity?

Please refer to question 3.5.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Maltese companies, partnerships, foundations, trusts and associations must identify and maintain a register of their ultimate beneficial owner/s ('UBO/s') as well as provide this information to, respectively: (i) the Registrar of Companies, in the case of companies and partnerships; (ii) the MFSA, in the case of trusts; and (iii) the Registrar for Legal Persons in the case of associations and foundations, that each maintain UBO registers. This information will be made available to the FIAU.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Payment service providers ('PSPs') are subject to the PMLFTR, which, in turn, mandate that any such entities adhere with the provisions of the Funds Transfer Regulation. Full information of the payer and payee – namely name, address and payment account number – must accompany all wire transfers, barring some exceptions. For example, if the PSPs of the originator and the beneficiary are both EU-based, the transfer need only be accompanied by the account number.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No. Ownership of shares is evidenced by their entry into a company's share register and by the issue of share certificates.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Generally, the PMLA/PMLFTR apply in a like manner to all the persons listed in question 3.1, which include certain non-financial institution businesses.

There are some exceptions, such as the privilege applicable to various professionals, including lawyers, which in turn are exempt from the duty to report suspicious transactions to the FIAU in accordance with Regulation 15(9) PMLFTR in certain instances. Some additional requirements are imposed on PSPs, which must comply with the Funds Transfer Regulation (refer to question 3.11 above). In addition, credit institutions must comply with the IPII for the banking sector, while gaming operators must comply with the IPII for the remote gaming sector and, or land-based casinos, as may be the case.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Aside from the business activities listed in question 3.1 above, there are no AML requirements applicable to other specific business sectors.

In terms of the IPI, customer risk and geographical risk are two of the factors that must be considered as part of a subject person's ML/FT risk assessment.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

On 30 October 2018, the FIAU published a revised version of the IPI for public consultation. The IPI are in the process of being revised in order to reflect the legislative amendments which took place between December 2017 and January 2018 to the PMLA/PMLFTR following the transposition of the 4AMLD and, more importantly, to provide more qualitative AML/CFT guidance reflecting today's technological reality. The newly proposed IPI may be viewed on the FIAU website. The public consultation closed on 31 December 2018. The definitive version of the IPI is expected to be published during the coming weeks.

The issuance of public consultations regarding sector-specific IPII for corporate services providers, the insurance sector, trustees and fiduciaries, is also expected in due course.

In addition, the MFSA launched its Vision 2021 in January 2019, which comprises a comprehensive strategy designed to clamp down on ML/FT in the financial services sector.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

As at October 2018, Malta features neither in the FATF's Public Statement nor in its Official Statement entitled 'Improving Global AML/CFT Compliance: On-going process', and is therefore deemed not to have any serious strategic weaknesses or deficiencies in the measures it implements for combatting AML/CFT.

In terms of MONEYVAL's 2012 Mutual Evaluation Report, Malta has been found to be 'Compliant' with 25 FATF 40 + 9 Recommendations, 'Largely Compliant' with 15, and 'Partially Compliant' with nine. Submission of follow-up reports led to the determination of Malta having a comprehensive AML/CFT legal structure, now also with enhanced criminal provisions to fight AML/CFT which have been largely brought in line with standards set by FATF requirements. As a result, Malta was removed from the follow-up and included, instead, in the 'biannual' update procedure.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The latest evaluation was carried out by MONEYVAL during a visit to Malta in November 2018, primarily to gauge Malta's level of compliance with the FATF 40 Recommendations and the level of effectiveness of Malta's AML/CFT system, as well as to provide recommendations as to how the country's AML/CFT regime could be strengthened. Results will be issued in the form of a Mutual Evaluation Report and adopted at MONEYVAL's 58th Plenary Meeting scheduled for July 2019.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Yes, all sources are available in English.

Reference is made to the website of the Ministry for Justice, Culture and Local Government (http://www.justiceservices.gov.mt/), where local legislation and regulations, including AML/CFT rules and regulations, may be accessed. In addition, the FIAU website enlists further information such as the IPI/IPII, additional guidance, FATF statements and MONEYVAL evaluations. The MFSA website (https://www.mfsa.com.mt/) also comprises substantial information on AML/CFT, including circulars and public consultations affecting the financial sector.

Dr. Emma Grech

City Legal
Britannia House, Suite 8
Old Bakery Street
Valletta
Malta

Tel: +356 2744 1120 / +356 2744 1121
Email: emma.grech@thecitylegal.com
URL: www.thecitylegal.com

Emma is a practising lawyer, having obtained her Doctor of Laws from the University of Malta in 2015 after submitting her thesis, entitled 'Regulating the Future? The Legal Implications of Social Games'. Thereafter, she embarked on an LL.M. in Banking and Finance Law at the University of London. Emma joined City Legal as a Legal Consultant in January 2018. Her main areas of practice at the firm are corporate finance and re-structuring, gambling and betting, anti-money laundering and data protection regulation. She advises on the legal and regulatory aspects of each of these areas, as well as the implications thereof on clients' business models. She frequently assists in a range of local and cross-border transactions involving her areas of specialisation. Emma also occupies the role of company secretary in various companies, including listed entities.

Dr. Christina Laudi

City Legal
Britannia House, Suite 8
Old Bakery Street
Valletta
Malta

Tel: +356 2744 1120 / +356 2744 1121
Email: christina.laudi@thecitylegal.com
URL: www.thecitylegal.com

Christina is an Associate at City Legal, and has been practising law with the firm since 2014 after having obtained her Doctor of Laws from the University of Malta in 2013. Her doctoral thesis was entitled 'Criminal Liability in Animal Welfare: A Comparative and Critical Analysis'. Following this, Christina read for an LL.M. in Family Law with the University of London, where she graduated in 2017. Christina's main areas of practice are family law, civil law, residence and immigration law as well as anti-money laundering regulation. Christina assists with various family law matters such as separation, divorce, care and custody issues as well as various civil law issues ranging from property law to damages and personal injury. Christina has also taken an active interest in the subject of financial crime and advises clients on matters of anti-money laundering regulation.

City | Legal

CITY LEGAL is a boutique law firm with offices in Valletta that has, throughout recent years, adopted an innovative approach focused at offering customised legal services in a manner which encourages its lawyers to combine specialist sector knowledge with a personalised service, resulting in the delivery of commercially-focused and high-quality legal advice.

Committed to this approach, the firm's lawyers consider themselves partners in their clients' businesses, taking pride in their clients' achievements, and constantly looking to establish strong, trusted, and lasting relationships with them.

We consider foreign-based law firms, corporate service providers, and other professionals including accountants, licensed trustees, tax advisers, and IT specialists to be our partners on the international front. Having ensured a regular overseas presence, the firm has established a robust international client-base which complements its local operations.

Chapter 23

Myanmar

Minn Naing Oo

Dr. Ei Ei Khin

Allen & Gledhill (Myanmar) Co., Ltd.

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The legal authority to prosecute money laundering offences under the Anti Money Laundering Law 2014 ("**AMLL**") rests with the Financial Intelligence Unit ("**FIU**"), a unit formed by the Central Board of Anti Money Laundering ("**Central Board**") pursuant to the AMLL to investigate and prosecute offences under the AMLL.

Section 68 of the AMLL prescribes that the prior sanction of the Central Board or organisation authorised by the Central Board shall be obtained to prosecute any offences under the AMLL.

As a matter of practice, the police will also need to be involved in any investigation under the AMLL.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The government must prove that the act committed falls within the meaning of "Money Laundering" and "Money Laundering" under Section 3(n) of the AMLL and it is defined as the commission of any of the following:

a) converting or transferring money or property, knowing or having reason to know that the money and property are obtained by illegal means, for the purpose of conventing or concealing the origin, or whether before or after the commission thereof, for the purpose of assisting a person involved in the commission of offence to evade the legal action under the AMLL;

b) changing the original nature, source, location and characteristics, or concealing or disguising the ownership or rights of money or property, knowing or having reason to know that the money and property are obtained by illegal means;

c) acquiring, possessing or using money or property, knowing or having reason to know at the time of receipt that money and property are obtained by illegal means; or

d) committing, attempting to commit, or conspiring with intention to commit, or by commission or omission, assisting, supporting, providing, managing, advising, being any member, and by any other means involving any offence mentioned in clause (a) to clause (c).

Section 5 of the AMLL defines the money laundering predicate offences as being the following:

a) offences committed by organised crimes;

b) offences relating to sexual exploitation including sexual exploitation of children;

c) offences relating to infringement of the Intellectual Property right;

d) offences relating to environmental crime;

e) offences relating to the evasion of tax and other tax crimes;

f) offences relating to piracy;

g) offences relating to terrorism;

h) offences relating to insider trading to get illicit profits by a person who is the first to know the information by using the said information himself or providing it to another person and market manipulation;

i) committing of any offence punishment with imprisonment for a term of a minimum of one year and above under any existing law of Myanmar;

j) offences prescribed by the Union Government that are applied to this Law by notification from time to time; and

k) offences relating to cooperation, abetting, supporting, providing, managing, advising and being the gang of commission of, committing or attempting to commit or conspiring to commit by action or omission of any offence contained in sub-sections (a) to (j) and by any other means.

Yes, tax evasion is a predicate offence for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Section 2 of the AMLL provides that the AMLL only applies to offences committed within the territories of the Union of Myanmar, or on board a vessel, an aircraft, and any motor vehicle registered under an existing law of Myanmar, or a Myanmar citizen or any person residing permanently in the Union of Myanmar who commits the said offence beyond the limits of the country.

There is extraterritorial jurisdiction only for Myanmar citizens or any person residing permanently in the Union of Myanmar or for an act committed on board a vessel, an aircraft, and any motor vehicle registered under an existing law of Myanmar.

Money laundering of the proceeds of foreign crimes is punishable only if it falls within the limits of Section 2 of the AMLL.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The relevant government authorities are the FIU, Scrutiny Body, Investigation Body and various law enforcement agencies in Myanmar (as set out below).

Chapter V of the AMLL provides that the FIU is the government authority responsible for investigating and prosecuting money laundering criminal offences.

The FIU shall, after receiving and scrutinising the reports and information under the AMLL, form and assign the Scrutiny Body which function is to scrutinise money laundering, financing of terrorism, money and properties obtained by illegal means and possession of terrorists pursuant to Section 14 of the AMLL. Further, an Investigation Body may also be formed by the Central Board to investigate the findings made in the report issued by the Scrutiny Body.

Further, law enforcement agencies in Myanmar which are responsible for detecting, investigating and scrutinising offences in Myanmar will also be responsible for the examination for compliance and enforcement of anti-money laundering requirements. Such law enforcement agencies include the Myanmar Police force, the Bureau of Special Investigation, Department of Customs and the Department of Immigration and National Registration.

1.5 Is there corporate criminal liability or only liability for natural persons?

Chapter XI of the AMLL on "*Offences and Penalties*" provides that there is both corporate criminal liability and liability for natural persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalty is imprisonment for a term which may extend to 10 years or in the case of a legal entity, a fine of 500 million Kyats.

1.7 What is the statute of limitations for money laundering crimes?

There is no period of limitation for criminal offences in Myanmar.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Enforcement is only at national level and there are no parallel state or provincial criminal offences for money laundering.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

No, there is no specific confiscation authority in Myanmar for an offence under the AMLL. A court order for confiscation of property is required for an offence under the AMLL. Under the AMLL, property subject to confiscation would include criminal proceeds and instruments of crime.

If there is no criminal conviction, confiscation is only possible on an administrative basis by the (i) Customs Department for money, bearer negotiable instruments, or precious stones or metals the value of which equals or exceeds an amount determined by the Central Board in his possession or baggage; or arranges for the transportation via mail or any type of vehicles into or out of Myanmar, which were not declared officially to the Customers Department by the person entering or leaving the territory of Myanmar, and (ii) Internal Revenue Department for property of corresponding value in the form of a pecuniary penalty order in tax evasion cases.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

No, we are not currently aware of any banks or other regulated financial institutions or other directors, officers or employees being convicted of money laundering.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions under the AMLL are resolved through the judicial process. Records of the fact of the judgments rendered by the court are public documents which can be procured from the courts. However, the terms of any settlements made are not publicly available.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The legal or administrative authorities are the Central Board and the Central Bank of Myanmar.

(i) Central Board

Pursuant to Section 7 of the AMLL, the Central Board is the authority in charge of laying down policies of anti-money laundering and terrorism financing in Myanmar. In this regard, the Central Board shall form the FIU which is the government authority responsible for investigating and prosecuting money laundering criminal offences. The FIU shall after receiving and scrutinising the reports and information it receives under the AMLL, form and assign the Scrutiny Body which function is to scrutinise money laundering, financing of terrorism, money and properties obtained by illegal means and possession of terrorists pursuant to Section 14 of the AMLL. Further, an Investigation Body may also be formed by the Central Board to investigate the findings made in the report issued by the Scrutiny Body.

Chapter VIII of the AMLL sets out the anti-money laundering requirements on Reporting Organisations (as defined under the AMLL). Such requirements include the requirement to:

a) carry out risk assessment of money laundering and terrorism financing;

b) carry out intermediary measures on accounts, customers and business relationships;

c) monitoring of complex or unusually large transactions or transactions with a person from a country which does not follow measures to prevent money laundering and terrorism financing;

d) maintain records; and

e) implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing.

"Reporting Organisations" is defined under the AMLL to mean "*banks and financial institutions, non financial enterprises and professions stipulated by this Law to report. In this expression, it also includes organisations which is assigned to report, by notification from time to time by the Central Control Board*".

(ii) Central Bank of Myanmar

Specifically, for banks and financial institutions, Directive No. (21/2015) on CDD Measures dated 2 October 2015 ("Directive") issued by the Central Bank of Myanmar also applies.

The Directive sets out additional obligations on banks and financial institutions (which supplement the requirements as set out in Chapter VIII of the AMLL) and such anti-money laundering requirements include the requirement to:

a) implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing;

b) carry out risk assessment of money laundering and terrorism financing;

c) customer due diligence;

d) ongoing monitoring of customer transactions;

e) suspicious transaction reporting; and

f) recordkeeping.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

We are not currently aware of any anti-money laundering requirements imposed by self-regulatory organisations or professional associations, to the extent they are publicly available.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The provisions of the AMLL are silent in this regard on the responsibility of the self-regulatory organisations or professional associations *vis-à-vis* their members. However, in general these self-regulatory organisations or professional associations do require that their members comply with all Myanmar laws (including the requirements and obligations under the AMLL) and may impose sanctions for failure to do so.

2.4 Are there requirements only at national level?

Yes, the requirements are only at national level and there are no specific state or regional level requirements.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see response to questions 1.4 and 2.1 above.

No, the criteria for examination are not publicly available.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the FIU is formed pursuant to the AMLL to investigate and prosecute offences under the AMLL.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no period of limitation for criminal offences in Myanmar.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Pursuant to Section 44 of the AMLL, failure to comply with the regulatory/administrative anti-money laundering requirements as listed in the response to question 2.1 above may attract a maximum penalty of imprisonment for a term which may extend to three years and may also be liable to a fine. If the offender is a company or organisation, one hundred million Kyats shall be imposed on such company or organisation.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Please see response to question 2.8 above which includes the maximum penalties of either imprisonment or fines under Chapter XI of the AMLL.

The other types of sanction are the confiscation orders or administrative orders that the Court is empowered to issue on properties and money relating to Money Laundering.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, the penalties are not only administrative/civil.

The violation of anti-money laundering obligations are also subject to criminal sanctions under Chapter XI of the AMLL. Please see response to question 2.8 above for more information.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

There are no administrative decisions under the AMLL Law. In general under Myanmar law, administrative decisions are subject to appeal under the specific rules of that administrative body.

Under the AMLL, only the court is able to impose penalties/sanctions and such judgments by the courts are publicly available.

Yes, financial institutions are able to appeal against any penalty assessment rendered in judicial proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Reporting Organisations (as defined under the AMLL) are the entities subject to anti-money laundering requirements.

"Reporting Organisations" is defined under the AMLL to mean "*banks and financial institutions, non financial enterprises and professions stipulated by this Law to report. In this expression, it also includes organisations which is assigned to report, by notification from time to time by the Central Control Board*".

The non-financial enterprises and professions stipulated under the AMLL to be Reporting Organisations are as follows:

"*a) Casinos;*

b) Real estate agents;

c) Dealers in precious metals and precious stones;

d) Lawyers, notaries, accountants or other independent legal professionals in respect of carrying out transactions acceptance and entrust of money and property of a client performing any of the following activities:

a. buying and selling immovable property

b. managing of client money, securities or other assets

c. management of bank, savings or securities accounts

d. organisation of contributions for the establishment, operation or management of companies

e. establishment of legal societies or arrangements, operation or management of companies

e) Company, control body and company service providers which as a business provide any of the following services to third parties:

a. acting as formation agent of legal persons

b. acting as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal society or arrangement persons

c. taking responsibility of a registration office, or business address, or correspondence or administrative address for a company, a partnership or any legal society arrangement

d. acting as a trustee in a trusteeship company or performing the equivalent function in any legal society arrangement

e. acting as a nominal shareholder or arranging a person to act as a nominal shareholder for another person".

Please see the answer to question 2.1 above for the obligations that Reporting Organisations are subject to.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

We are not currently aware of any rules or regulations under Myanmar law which apply the anti-money laundering requirements to the cryptocurrency industry.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes, Reporting Organisations are required to implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing pursuant to Section 28 of the AMLL.

The required elements of such internal programmes, policies, procedures and controls are as follows:

"*a) intermediary measures, continuous focus investigation, monitoring the transactions, the obligations to report and to maintain the record;*

b) supervising the procedures to ensure high standard of integrity of its service and a system to evaluate the personal, servicing and historical background of financial of these services;

c) continuous training programmes to assist by specific in respect of knowing their intermediary, recognising the specific responsibilities related to the anti money laundering and counter financial terrorism and transferring which are required to report contained in chapter 8;

d) an independent audit function to examine compliance with and effectiveness of the measures of taken action in implementing this Law."

Further, for banks and financial institutions, Clause 4 of the Directive is applicable and such internal programmes, policies, procedures and controls should address the following requirements:

"*a) Risk assessment of the customer as well as transactions;*

b) Identification and verification of the customer, including walk-in/occasional customers, beneficial owners;

c) Application of customer due diligence measures to customers;

d) Exercising ongoing customer due diligence measures in relation to business relations and transactions;

e) Application of enhanced customer due diligence measures to high risk customers, including politically exposed persons;

f) Maintaining records and information of customers and transactions;

g) Monitoring transactions set out in section 21 of the AMLL;

h) Reporting to the Financial Intelligence Unit of transactions as set out in section 32 and 34 of the AMLL;

i) Ensuring that internal policies, procedures, systems and controls are subject to independent audit function and review;

j) The appointment of a compliance officer at senior management level to ensure compliance with the provisions of the AMLL, Rules issued the AMLL and the Directive;

k) Ensuring high standards of integrity while recruiting employees;

l) Providing an on-going training program to all new and existing employees, directors, board members and executive or management staff;

m) Other arrangements as prescribed by the CBM and competent regulatory authorities."

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Recordkeeping

The requirements for such recordkeeping are as set out in Section 23 of the AMLL and Reporting Organisations are required to maintain records of the following:

"*a) evidence documents, records obtained from intermediary measure and finding documents including accounts and business correspondence of intermediary or beneficial owners for at least five years after the business relationship has been ceased or the occasional transaction has been carried out;*

b) records on attemption of transaction in both domestic and foreign or records on transaction for the following five years after the transaction has been carried out;

c) copies of transaction reports under Chapter 8 of this law and other related documents for at least five years from the date of the report was submitted to the Financial Intelligence Unit; and

d) risk assessment and other underlying information for a period of five years from the date of its completion or update."

Further, for banks and financial institutions, Clause 58 of the Directive is applicable and copies of all records obtained through the customer due diligence process will need to be maintained.

Reporting

Section 32 of the AMLL provides that Reporting Organisations shall *promptly* report to the FIU if the amount of transaction is equal to or exceeds the designated threshold of US$10,000 or it has reasonable grounds to believe that any money or property is obtained by illegal means or is related to money laundering or terrorism financing or an attempt to do so. Please also note that Reporting Organisations are required to submit a suspicious transaction report to the FIU for suspicious transactions that may be an offence relating to money laundering or financing of terrorism. In addition, the FIU collects a wide range of transaction data (in addition to the aforementioned suspicious transactions report) including immovable property transactions, cash transactions and gems purchasing data from a wide range of Reporting Organisations. Despite the obligation to file these reports, only banks had filed the suspicious transactions report thus far and threshold reports are reports are rarely reported by other sectors.

Further for banks and financial institutions, Clause 47 of the Directive is applicable and a cross-border wire transfer in excess of US$10,000 or a domestic wire transfer in excess of 100 million Kyats will need to be reported to the FIU by either the ordering bank or beneficiary bank. Clause 49 of the Directive prescribes that banks or financial institutions should report to the FIU within 24 hours if it is situated in an urban area or within three days if it is situated in a remote area.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Reporting Organisations are required to submit a suspicious transaction report to the FIU for suspicious transactions that may be an offence relating to money laundering or financing of terrorism. Such suspicious transaction reports should be submitted to the FIU within 24 hours if it is situated in an urban area or within three days if it is situated in a remote area.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

For banks and financial institutions, Clause 47 of the Directive is applicable and a cross-border wire transfer in excess of US$10,000 will need to be reported to the FIU by either the ordering bank or beneficiary bank. Clause 49 of the Directive prescribes that banks or financial institutions should report to the FIU within 24 hours if it is situated in an urban area or within three days if it is situated in a remote area.

This report should be in the form as prescribed under the AMLL as set out at Form 7 of the Anti Money Laundering Rules 2015.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Pursuant to Section 19(d) of the AMLL, Reporting Organisations are to undertake the following customer due diligence measures:

"*a) identifying the intermediary by means of free and reliable sources, documents, data or information and verifying the intermediary's registration;*

b) Collecting and understanding the purpose of business relationship and the nature of information;

c) Identifying the main beneficiary to be verified that the reporting organizations may know who is the main beneficiary and understand possession and control of company or legal arrangement and taking the suitable measures in order to verify the evidence of the said beneficiary;

d) Verifying whether the person on behalf of intermediary is authorised person or not for person, company. organisation or legal arrangements and verifying the registration of that person is correct; verifying the legal status of person, company, organisation or legal arrangement; receiving information of intermediary's name, legal formation, address and directors and regulating the power to be bound to company or legal arrangements;

e) Enhancing customer due diligence measures contained in clauses (a) to (d) if it has reasonable grounds to believe that the customer is a domestic and foreign politically exposed person or international politically exposed person."

For banks and financial institutions, Clause 11 of the Directive is applicable and additional customer due diligence as follows would be required:

a) regarding natural persons, the Reporting Organisation must verify the identity of their customers using reliable, independent source documents, data, or information as outlined in Schedule 1 of the Directive; and

b) regarding legal persons or legal arrangements, the Reporting Organisation must obtain and verify the information required using reliable, independently sourced documents, data, or information as outlined in Schedule 1 of the Directive.

In brief, Schedule 1 of the Directive sets out certain specified information that banks and financial institutions would be required to collect from their customers.

Further, enhanced customer due diligence is required for higher risk customers as set out in Clause 17 of the Directive.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Clause 35 of the Directive provides that banks and financial institutions shall not enter into or continue a correspondent or business relationship with a shell bank or a correspondent financial institution in a foreign country that allows its accounts to be used by a shell bank.

3.9 What is the criteria for reporting suspicious activity?

There is no specified criteria but a suspicious transaction report is to be made if there are reasonable grounds to believe that a transaction or attempted transaction is money or property obtained by illegal means or is related to money laundering or terrorism financing.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The Directorate of Investment and Company Administration, the registrar of companies in Myanmar, has set up an online registry, MyCo which functions as a public registry of all companies and entities registered in Myanmar under the Myanmar Companies Law 2017. Information on shareholding and director appointment can be accessed on MyCo.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, Clause 38 of the Directive prescribes that accurate originator and recipient information be included on the wire transfer.

Yes, such information should remain with the wire transfer and related messages throughout the payment chain.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Share certificates are *prima facie* evidence of the title of shares and the Myanmar Companies Law 2017 requires that a share certificate be issued to shareholders within 28 days of the allotment of shares.

A shareholder is recognised to be a shareholder of a company when such shareholder's name is indicated in the company's register of members.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Please see the answer to question 2.1 above.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No, as disclosed above, we are not currently aware of any anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

We are not currently aware of any additional anti-money laundering measures being contemplated or are under consideration.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The last review conducted by the Asia/Pacific Group on Money Laundering from 20 November to 1 December 2017 stated that Myanmar is non-compliant with certain recommendations of the FATF, in particular on the following:

a) Recommendation 7 – Targeted Financial sanctions related to proliferation.

b) Recommendation 14 – Money or value transfer services.

c) Recommendation 19 – High-risk countries.

d) Recommendation 24 – Transparency and beneficial ownership of legal persons.

e) Recommendation 25 – Transparency and beneficial ownership of legal arrangements.

f) Recommendation 28 – Regulation and supervision of DNFBPs.

The above recommendations of the FATF do not currently form part of the AMLL and in order to comply with these recommendations, the main impediment would be having the legislative support to pass such legal reform.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The last review was conducted by the Asia/Pacific Group on Money Laundering from 20 November to 1 December 2017.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

This can be obtained from the FIU website at https://mfiu.gov.mm/en.

English translations are available.

Minn Naing Oo

Allen & Gledhill (Myanmar) Co., Ltd.
Junction City Tower, #18-01
Bogyoke Aung San Road
Pabedan Township
Yangon
Myanmar

Tel: *+95 1 925 3719*
Email: *minn.naingoo@allenandgledhill.com*
URL: *www.allenandgledhill.com/mm*

Minn is the Managing Director of Allen & Gledhill (Myanmar) and a Partner of Allen & Gledhill. He has extensive experience advising on banking and finance, mergers and acquisitions, infrastructure projects, corporate and commercial, arbitration and competition. He has acted for multinational corporations, multilateral agencies, financial institutions, private equity funds and Myanmar conglomerates.

He was previously the Chief Executive Officer of the Singapore International Arbitration Centre and Director at the Ministry of Trade and Industry Singapore. He is also a Fellow of the Chartered Institute of Arbitrators and the Singapore Institute of Arbitrators, and has been appointed to dispute panels for disputes between World Trade Organisation (WTO) Member States.

Minn graduated from the National University of Singapore with an LL.B. in 1996. He was called to the Singapore Bar in 1997, and he obtained an LL.M. in 2001 from Columbia University as a Harlan Fiske Stone Scholar.

Dr. Ei Ei Khin

Allen & Gledhill (Myanmar) Co., Ltd.
Junction City Tower, #18-01
Bogyoke Aung San Road
Pabedan Township
Yangon
Myanmar

Tel: *+95 1 925 3717/3718*
Email: *eiei.khin@allenandgledhill.com*
URL: *www.allenandgledhill.com/mm*

Dr. Ei is a Consultant of Allen & Gledhill (Myanmar). Her experience focuses on commercial litigation and international arbitration.

She has extensive research works and experience in commercial litigation, and advising on and being involved in various regulatory fields on behalf of the Supreme Court of the Union of Myanmar.

Prior to joining Allen & Gledhill (Myanmar), she was a Judicial Officer at the Supreme Court and a Judge at the township and district level of courts in Yangon and Mandalay, handling civil, criminal and juvenile cases. She was a head of office at the Office of the Chief Justice, High Court of Mandalay, and was also Deputy Director at the Supreme Court of the Union of Myanmar, where she was a member of the legal drafting committee of the Supreme Court and leader of the Working Group on the drafting of the new Arbitration Law, IP Laws and Insolvency Law.

She graduated from Yangon University with LL.B. and LL.M. degrees and holds a PhD from Niigata University, Japan.

ALLEN & GLEDHILL

Allen & Gledhill (Myanmar) is the local Myanmar office of one of South-east Asia's leading and largest law firms, Allen & Gledhill. Based in Yangon, we are a fully licensed law firm which provides Myanmar legal and tax advice, and issues Myanmar legal opinions. Our Firm, staffed by local and foreign qualified lawyers, is supported by the network of Allen & Gledhill and combines sound local knowledge with best international practices to provide value-added advice and unparalleled service to our clients. Led by Minn Naing Oo, a Singapore and New York qualified lawyer fluent in the Myanmar language, Minn has well-established connections in the Myanmar business community and experience in advising both foreign investors and local businesses on their projects in Myanmar.

Operational since 2014, Allen & Gledhill (Myanmar) has gained an excellent reputation for advising local conglomerates and organisations as well as international clients across diversified industry sectors and has been recognised as a leading law firm by notable legal directories including *IFLR1000*, *Chambers Asia-Pacific* and *The Legal 500 Asia Pacific*.

Netherlands

Jurjan Geertsma

Madelon Stevens

JahaeRaymakers

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Dutch Public Prosecution Service (**DPPS**, *Openbaar Ministerie*).

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Under Dutch criminal law, the substantive standard can be generally described as the prohibition of conducting acts with regard to objects that – directly or indirectly – originate from a crime. According to Title XXXA of the Dutch Penal Code (**DPC**, *Wetboek van Strafrecht*), the prohibited acts are, amongst other things:

- Hiding or concealing:
  - the actual origin, finding place, disposal or transfer of the object; and
  - who the entitled person to an object is or who the person is that possesses the object.
- The acquisition, possession, transfer, conversion and use of an object that originates from a crime.

Please note that the term 'object' also covers property rights.

The DPC distinguishes the following types of money laundering:

- Intentional money laundering (Article 420*bis* DPC) (conditional intent regarding the origin of the object suffices).
- Habitual money laundering (Article 420*ter* DPC) (heaviest form, intentional money laundering on a regular basis).
- Money laundering as a regular occupation or business activity (Article 420*ter* DPC).
- Culpable money laundering (Article 420*quater* DPC) (lower limit, culpa regarding the origin of the object suffices).
- Simple money laundering (Article 420*bis* 1 and 420*quater* 1 DPC) (acquisition or possession of an object that originates directly from an own crime) (both the intentional and culpable form are criminalised).

The object that is being laundered must originate from a previous crime (*misdrijf*). It is not required that the object originates entirely from a crime: according to Dutch case law, an object that is also partly financed with criminal money and partly with legal money is being considered to originate from a crime ("mixture"). Objects obtained through violations (*overtredingen*) fall outside the scope of money laundering under Dutch law.

Predicate offences can be all crimes whereby an object has been acquired, including tax evasion.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In general, the DPC provides jurisdiction for the DPPS to prosecute suspects for criminal offences if the case has a link with the Netherlands, for instance if a Dutch person commits a crime abroad (as long as the act is punishable in the foreign country as well) or if the crime has been committed partially on Dutch territory.

In terms of jurisdiction, the DPC does not provide for a limitation in predicate offences. Therefore, the DPPS has jurisdiction to prosecute suspects for money laundering in the Netherlands of objects that originate from crimes committed and is punishable abroad.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The DPPS, assisted by the Dutch police and Fiscal Intelligence and Investigation Service (*FIOD*).

1.5 Is there corporate criminal liability or only liability for natural persons?

According to Article 51 of the DPC, both individuals and legal entities are capable of committing criminal offences. It follows from Dutch case law that a legal entity can be held criminally liable for criminal offences of individuals (for instance employees) if these offences can be 'reasonably attributed' to the legal entity, which depends on the specific facts and circumstances of the case. According to the Dutch Supreme Court, an important point of reference in this context is whether the offence (of the individual) took place within the 'sphere' of the legal entity.

Furthermore, according to Article 51 of the DPC, if criminal liability of the legal entity has been established, individuals that ordered the commission of the criminal offence (*opdrachtgever*) or actually directed the unlawful behaviour (*feitelijk leidinggever*) may also be prosecuted and convicted for such criminal offences.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Depending on the type of money laundering as discussed in question 1.2, the maximum penalties for individuals vary from:

- Imprisonment: three months (simple culpable money laundering) to eight years (habitual money laundering).
- Fines: EUR 20,750 to EUR 83,000.

The maximum penalties for legal entities (fines only) vary from EUR 83,000 to 10 per cent of the annual turnover of the previous fiscal year.

1.7 What is the statute of limitations for money laundering crimes?

According to Article 70 DPC, depending on the type of money laundering as discussed in question 1.2, the statute of limitations varies from six years (culpable money laundering and simple money laundering) to 20 years (habitual money laundering).

In addition, Article 72 DPC states that after any act of prosecution the statute of limitations starts over. The absolute statutes of limitations for the aforementioned money laundering crimes varies from 12 to 40 years (two times the initial statute of limitations).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

In general, we see a development in which the cooperation between Dutch and foreign authorities in cross-border criminal cases increases. A recent matter concerns the investigation of the DPPS to money laundering by the Dutch ING Bank in relation to corrupt payments made by telecom company Vimpelcom to, amongst others, the daughter of the former president of Uzbekistan, Gulnara Karimova, for which the bank reached an out-of-court settlement with the DPPS.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The DPPS has the power to forfeit and confiscate objects.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

We are familiar with a few cases in which (small) financial institutions or their directors have been convicted of money laundering. In addition, the DPPS seems to increase its focus on so-called gate-keepers, especially large(r) financial institutions. For instance, in 2018 the DPPS conducted a criminal investigation to ING bank in relation to money laundering in the *VimpelCom*-case. The bank reached a settlement with the DPPS for violation of the Money Laundering and Terrorist Financing (Prevention) Act (*Wwft*) and culpable money laundering. According to the DPPS, the bank did not prevent the bank accounts of ING customers in the Netherlands from being used to launder hundreds of millions of euros between 2010 and 2016. ING paid a fine of EUR 775,000,000.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

In almost all large (international) fraud cases that occurred so far, the DPPS has reached an out-of-court settlement (*transactie*) with suspects, in which settlements included the term of paying a certain fine.

The policy of the Dutch Public Prosecutors Office regarding high and special transaction ("*Aanwijzing hoge transacties en bijzondere transacties*") states that in principle a press release will be published for settlements of EUR 50,000 or more or special settlements between EUR 2,500 and EUR 50,000. Such a press release in any case includes the following information: a description of the criminal offences which according to the DPPS can be proven; a detailed prescription of the proposed settlement with respect to all involved suspects (specifically in case of a suspected legal entity and responsible individuals); a description of the underlying considerations with regards to the settlement (including a motivation of why the case should not be brought for a criminal judge); and an explanation of the amount of the fine.

The ING-settlement was followed by a press release from the DPPS including a reference to the settlement agreement and a statement of facts (*feitenrelaas*).

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Depending on the type of financial institution as mentioned in Article 1a Wwft, the authorities for imposing anti-money laundering requirements are:

- The Dutch Central Bank (**DNB**): regulator for banks; credit institutions; exchange institutions; electronic money institutions; payment institutions; life insurers; trust offices; and lessees of safes.
- The Dutch Authority for the Financial Markets (**AFM**): regulator for investment firms; investment institutions; and banks and financial service providers insofar as they mediate in life insurance policies and institutions for collective investment and securities (**UCITS**).
- The Financial Supervision Office (**BFT**): regulator for accountants; tax advisers; and notaries.
- The Dutch Tax Authority and Wwft Supervision Office: regulator for real estate agents or intermediaries; valuers; traders/sellers of goods; pawnshops; and domiciles.
- The local Dean of the Bar Association: the regulator for lawyers (attorneys-at-law).
- The Gaming Authority (**KSA**): regulator for gaming casinos.
- The Investigation and enforcement services & intelligence and security services: Financial Intelligence Unit (authority where institutions must report unusual transactions); and the DPPS (authority to investigate unusual transactions and other alleged criminal violations of the Wwft).

The Wwft comprises five core obligations:

- Taking measures to identify and assess its risks of money laundering and terrorist financing, including the recording of the results of such assessment. In addition, the obligation

exists to have policies and procedures in place to mitigate and effectively manage the risks of money laundering and terrorist financing and the risks identified in the national and supranational risk assessment (Articles 1f–2d Wwft).

- Conducting a thorough – standard, simplified or strengthened – customer due diligence (**CDD**) prior to entering into a business relationship or conducting (incidental) transactions (Articles 3– 11 Wwft).
- Reporting of unusual transactions with the Financial Intelligence Unit, on the basis of objective or subjective indicators (Articles 12–23a Wwft).
- Providing periodic training to employees in order for them to be able to recognise unusual transactions and conduct a proper and comprehensive CDD (Article 35 Wwft).
- Adequate record-keeping of risk assessment/client due diligence and reporting of unusual transactions and providing these results to regulators upon request (Articles 33–34 Wwft).

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Most of the authorities mentioned in question 2.1 (of which some are self-regulatory organisations such as the local Dean of the Bar Association) provide guidelines for the Wwft institutions in order to assist them in complying with the obligations of the Wwft. However, the authorities do not impose additional requirements.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The authorities mentioned in question 2.1 are responsible for anti-money laundering compliance and enforcement against the Wwft institutions that fall under their responsibility.

2.4 Are there requirements only at national level?

Since the Wwft obligations are implementations of the requirements as set by the European AML-Directives, the Wwft obligations stem from international level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see questions 2.1 and 2.2. Please note that the guidance provided are not always up to date or very clear.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

According to the Wwft, the Dutch Financial Intelligence Unit is the only and central reporting point where the Wwft institutions must report unusual transactions.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Enforcement of the Wwft can take place via administrative measures, such as an order subject to an incremental penalty (*last onder dwangsom*) in order to stop the institution of violating the Wwft or an administrative penalty (*bestuurlijke boete*). The statute of limitations for an administrative penalty is five years from the day of the violation.

In addition, violation of (one or more of) the five core obligations as discussed in question 2.1 can constitute a criminal offence under the Economic Crimes Act (**WED**, *Wet op de economische delicten*) for which the DPPS can start prosecution. According to Articles 1, 2 and 6 of the WED in conjunction with Articles 70 and 72 of the DPC, the absolute statutes of limitations vary from six years (in the case of a culpable violation) to 24 years (in the case of a habitual and intentional violation).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Administrative penalties: for most violations of the aforementioned five core obligations of the Wwft, the assigned regulator can impose administrative penalties that may vary from EUR 10,000 (minor violation) to EUR 4,000,000 (serious violation). The maximum penalty for banks, trust offices and a few other financial institutions such as investment firms amounts to EUR 5,000,000. In case of recidivism within five years from a previous violation, the administrative penalty can be twice the aforementioned amounts. In addition, in case of serious violations by banks, trust offices and a few other financial institutions, the Wwft provides for administrative penalties up to 20 per cent of the net turnover of the previous fiscal year.

Criminal penalties: the maximum penalties for violations of the aforementioned five core obligations of the Wwft vary from six months to four years' imprisonment or fines ranging from EUR 20,750 to EUR 83,000 for natural persons. The maximum penalties for legal entities (fines only) vary from EUR 83,000 to 10 per cent of the annual turnover of the previous fiscal year.

In addition, the WED prescribes that if the value of the goods with which or with regard to which the crime has been committed, or which has been wholly or partly obtained through the crime, is higher than the fourth part of the maximum of the fine which can be imposed, a fine of the next higher category may be imposed.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The WED in conjunction with the DPC can impose various additional penalties (*bijkomende straffen*) such as removal from holding offices for a certain period and total or partial cessation of the entity of the convicted person where the crime was committed. In addition, certain measures (*maatregelen*) can be imposed, such as deprivation of the unlawfully obtained advantage.

In addition, the Wwft provides for the obligation of regulators to publish administrative fines in certain cases.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Please see the answers to questions 2.8 and 2.9 above.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

Judicial proceedings in the Netherlands are public.

If an institution gets convicted of criminal violations of the DPC or Wwft by a District Court, it can appeal such verdict to the Court of Appeal. In case of a conviction by the Court of Appeal in criminal proceedings, an institution can under certain circumstances appeal to the Supreme Court, which has the competence to set aside or affirm rulings of lower courts, but no competence to re-examine or question the facts. The Supreme Court only considers whether the lower courts applied the law correctly and the rulings have sufficient reasoning.

In administrative proceedings, an institution must first file a complaint (*bezwaar*) with the administrative body imposing the sanction, followed by an appeal before the court. Under certain circumstances, a possibility to appeal against a ruling by the court with the Commission for Appeal for business and industry exists.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Article 1a Wwft distinguishes three main categories of "institutions", namely:

1) Banks.
2) Other financial institutions:
   a. Investment institutions.
   b. Investment firms.
   c. Mediators in life insurance.
   d. Payment service agents.
   e. Payment service providers acting on behalf of a payment service provider with another EU member state licence.
   f. Payment service providers.
   g. Electronic money institutions.
   h. Institutions for collective investment and securities (UCITS).
   i. Institutions not being a bank that nevertheless carries out banking activities.
   j. Life insurers.
   k. Landlords of safes.
   l. Currency exchange offices.
3) Designated natural persons or legal entities acting in the context of their professional activities:
   a. Accountants.
   b. Lawyers.
   c. Tax advisers.
   d. Domicile providers.
   e. Traders/sellers of real estate, vehicles, ships, art objects, antiques, precious stones, precious metals, or jewellery.
   f. Brokers or intermediaries in matters of great value (EUR 10,000 or more).
   g. Notaries.
   h. Pawnshops.
   i. Gaming casinos.
   j. Appraisers.
   k. Trust offices.

With regard to lawyers and (junior) notaries, the Wwft is only applicable if they:

1. independently provide professional or professional advice or assistance with:
   i. the purchase or sale of registered goods;
   ii. managing money, securities, coins, notes, precious metals, precious stones or other values;
   iii. the establishment or management of companies, legal persons or similar bodies as referred to in Article 2, first paragraph, part b, of the General Government Tax Act;
   iv. the purchase or sale of shares in, or the total or partial purchase or sale or takeover of companies, companies, legal persons or similar bodies as referred to in Article 2, first paragraph, under b, of the General Government Tax Act;
   v. activities in the field of taxation that are comparable to the activities of the professional groups described in part a; and
   vi. establishing a mortgage right on registered property; or
2. act independently, professionally, or commercially in the name and on behalf of a client in any financial transaction or real estate transaction.

The Wwft does not apply to tax advisers, lawyers and notaries, insofar as they perform work for a client regarding the determination of his legal position, his legal representation and defence, giving advice before, during and after legal proceedings, or giving advice on instituting or avoiding legal proceedings.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Dutch regulators AFM and DNB have advised the Dutch Minister of Finance to (i) introduce a licensing regime for fiat-crypto exchange platforms and crypto wallet providers, to ensure effective implementation of the revised European anti-money laundering directive, and (ii) advocate for the amendment of the European regulatory framework to enable blockchain-based development of SME funding, and reconcile the national and the European regulatory definitions of security.

A legislative proposal is currently pending to bring virtual currency under the scope of the Wwft.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

As discussed in question 2.1, the Wwft comprises five core obligations that Wwft instututions are required to meet. It is up to the Institutions themselves to decide on how they implement such obligations. Dutch law does not provide for an obligation to maintain specific compliance programmes.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Recordkeeping: a Wwft institution has to keep records of:

- the performed client due diligence on the basis of the Wwft; and
- the measures it took to investigate complex and unusually large transactions.

Article 33 Wwft states that the institution must keep these records for five years from the date of termination of the business relationship or the date the transaction has been executed.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

According to Article 16 of the Wwft, an institution is obliged to immediately (but in any case within two weeks) report an unusual intended or effected transaction with the FIU, right after it became aware of the unusual nature of the transaction. The reporting obligation also applies if:

- a CDD failed and there are also indications that the customer concerned is involved in money laundering or terrorist financing; or
- a business relationship is terminated and there are also indications that the customer concerned is involved in money laundering or terrorist financing.

In order to determine the nature of the transaction, the *Uitvoeringsbesluit Wwft 2018* provides for objective and subjective indicators for specific Wwft institutions. Objective indicators for banks and some other financial institutions are for instance (cash) transactions of EUR 10,000 or more or money transfer of EUR 2,000 or more. Subjective indicators are more vague. A frequently used subjective indicator is, for instance, if a transaction gives reason for the institution to assume that it may be related to money laundering or terrorist financing.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Though Dutch law is not very clear on this point, the Wwft does not seem to provide for a territorial delineation of unusual transactions as such. The parliamentary history of the Wwft and Dutch caselaw seem to suggest that foreign transactions may also be subject to the reporting requirements of Article 16 Wwft. Therefore, Wwft institutions can also be obliged to report cross-border transactions, if such transactions are considered to be unusual, as discussed in question 3.5.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

As discussed in question 2.1, the Wwft provides for three types of CDD: standard; simplified; or strengthened CDD. All types of due diligence need to be conducted prior to entering into a business relationship or conducting (incidental) transactions (Articles 3–11 Wwft).

The type of CDD an institution needs to conduct in a specific case entirely depends on the type of client and transaction. The starting point is that an institution conducts a standard CDD, unless a business relationship or transaction by its nature entails a low risk of money laundering or financing of terrorism. In that case, a simplified due diligence suffices. If a business relationship or transaction by its nature entails a high risk of money laundering or financing of terrorism, the institution must conduct a strengthened due diligence. This is also the case if the state where the customer is domiciled or established or has its seat has been designated by the European Commission as a state with a higher risk of money laundering or terrorist financing on the basis of Article 9 of the fourth Anti-Money Laundering Directive.

Where a risk on money laundering or financing of terrorism in a specific case exists a background check of the customer, identification of the UBO and the purpose and nature of the business relationship, amongst others, will also need to be determined.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

According to Article 5 Wwft, it is prohibited for banks and other financial institutions to enter into or continue a correspondent relationship with a shell bank or with a bank or other financial institution that is known to allow a shell bank to use its accounts.

3.9 What is the criteria for reporting suspicious activity?

Please see question 3.5. Please note that in the Netherlands unusual activities should be reported.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

As of March 2019, the Netherlands has still not fully implemented the fourth Anti-Money Laundering Directive. Consequently, there is no register for Ultimate Beneficial Owners to date.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

We refer to the DNB guidance that describes the following:

FATF Special Recommendation VII on wire transfers stipulates that electronic transfers must contain certain information about the party instructing the payment. In Europe, this FATF Recommendation has been transposed into Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying the transfer of funds. The Regulation has direct effect in the Netherlands. The Wwft stipulates that a customer due diligence must be performed whenever an

institution effects a non-recurring transaction into or out of the Netherlands on behalf of a customer or a trust that involves a transfer of funds as referred to in Section 2(7) of the Regulation.

The Regulation lays down rules concerning the information on the payer that must accompany the transfer of funds in order to ensure that the authorities responsible for combatting money laundering and terrorist financing have direct access to basic information that can help them exercise their duties. Institutions will generally have access to this information from the customer due diligence. The institution also performs a customer due diligence when executing a nonrecurring transaction into or out of the Netherlands on behalf of a customer or trust which is affecting a transfer of funds.

Full information about the payer comprises:

- Name.
- Address (or date and place of birth, customer identification number or national identity number).
- Account number (if this is not available, replace it with a unique identification code that can be used to trace the payer).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Yes, ownership of legal entities in the form of bearer shares is permitted. However, some of the regulators mention in their guidance that the fact that a customer holds bearer shares could be a reason for a high risk approach and should be indicated as a red flag for money laundering.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes, we refer to the list provided in question 3.1 which describes that non-financial institutions are also considered to be Wwft institutions to whom the Wwft core obligations apply, for instance natural persons or legal entities acting in the context of their professional activities:

a. traders/sellers of real estate, vehicles, ships, art objects, antiques, precious stones, precious metals, or jewellery; and
b. brokers or intermediaries in matters of great value (EUR 10,000 or more).

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Please see question 3.13 above.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

A part of AMLD 4 still has to be implemented. AMLD 5 still has to be implemented in whole.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Please see question 4.1 above. The last FATF evaluation is from 2014 and therefore is no longer up to date.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The FATF has evaluated the anti-money laundering regime of the Netherlands. For further information please see: http://www.fatf-gafi.org/documents/documents/fur-netherlands-2014.html.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

For English publications we refer to:

- The website of the FIU: https://www.fiu-nederland.nl/en.
- DNB Guidance on the Wwft: http://www.toezicht.dnb.nl/en/bin aries/51-212353.pdf.
- The Fifth European Anti-Money Laundering Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A3 2018L0843.

Jurjan Geertsma

JahaeRaymakers
Mondriaantoren, 19th floor
Amstelplein 40
1096 BC Amsterdam
Netherlands

Tel: *+31 20 435 25 25*
Email: *geertsma@jahae.nl*
URL: *www.jahae.nl*

Jurjan Geertsma's legal practice focuses expressly on disciplinary law, the law of sanctions and the reputational issues involved. He helps his clients to identify potential risks, jointly draws up an appropriate strategy, and proactively and resolutely goes in search of solutions. He assists companies from a wide range of sectors (including the chemical, food and property sectors), financial institutions (such as trust offices) and professional practitioners (e.g., the healthcare sector and the notarial and accountancy practices) who are faced with criminal accusations, administrative enforcement, and supervisory and disciplinary issues. Jurjan is a member of the Dutch Association of Defence Counsel (**NVSA**) and the European Criminal Bar Association (**ECBA**), where he forms part of the Anti-Corruption Working Group. He is also involved in the Corporate Responsibility & Anti-Corruption Commission of the International Chamber of Commerce **(ICC**), and the Asset Tracing & Recovery working group of the Institute for Financial Crime (**IFFC**). He teaches courses at institutions, for professional practitioners and for legal and compliance officers in the fields of Anti Money Laundering (**AML**), Anti Bribery & Corruption (**ABC**), International Sanctions Regulations and Compliance, Integrity, Client Confidentiality and Lawyer-Client Privilege, and organises interrogation and search ('mock dawn raid') training sessions.

Madelon Stevens

JahaeRaymakers
Mondriaantoren, 19th floor
Amstelplein 40
1096 BC Amsterdam
Netherlands

Tel: *+31 20 435 25 25*
Email: *stevens@jahae.nl*
URL: *www.jahae.nl*

Madelon Stevens specialises in financial, economic and tax sanctions law. She advises and assists legal entities, banks and other financial institutions (managing directors and/or supervisory directors) that are faced with (imminent) supervision or enforcement issues under administrative or criminal law, e.g., involving matters of corruption, (tax) fraud, forgery, bribery, money laundering or compliance with environmental and working conditions legislation. Madelon also has experience in organising and conducting internal investigations. She frequently advises on compliance and integrity issues, particularly in the field of Dutch and international anti-corruption and anti-money-laundering regulations (under the Dutch Money Laundering and Terrorist Financing (Prevention) Act). Furthermore, she organises training sessions, e.g., on how to act in the event of an investigation or dawn raid by supervisory authorities or law enforcement agencies. Madelon is a board member of the NVJSA (Dutch Association of Young Criminal Lawyers) and member of the Women's White Collar Defence Association.

Jahae Raymakers®
risks, reputations & sanctions

JahaeRaymakers is a leading niche firm with 10 lawyers. The firm specialises in risk & reputation management, supervision & enforcement, law of sanctions and European & international proceedings. Its lawyers act as trusted advisors for a wide range of public authorities, (listed) companies, museums and their directors, and high-profile and other private individuals. They have detailed knowledge, a wealth of experience and an excellent international network.

Trust, discretion, quality and determination are paramount in the often sensitive cases handled by JahaeRaymakers. The firm's aim is to adequately solve all cases. Whenever possible, it looks to take action before problems occur, preferably in the background and out of court. Where necessary, the firm does battle in court to achieve the best possible outcome for all its clients.

Peru

Ljubica Vodanovic

Adolfo Morán

Vodanovic Legal

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Public Prosecutor's Office is the legal authority responsible for investigating and prosecuting individuals that are accused of committing money laundering. Within the Public Prosecutor's Office, there is a specialised team of prosecutors focused on money laundering crimes.

Additionally, the Financial Intelligence Unit (FIU), which is part of the Superintendence of Banking and Insurance (SBS, in Spanish), is the legal authority entitled to receive and analyse financial information in order to determine if there are suspicious activities related to money laundering and if this is the case, to inform to the Public Prosecutor's Office about its findings.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Money laundering is a criminal offence regulated in the Legislative Decree N° 1106. There are three modalities of money laundering:

1. When a person converts or transfers money, goods, effects or profits that he knows or should have presumed that they had illicit origins, with the purpose to evade the identification of such illicit origin.
2. When a person acquires, utilises, possesses, stores, manages, receives, hides or keeps with him money, goods, effects or profits that he knows or should have presumed they had illicit origins.
3. When a person transports or moves cash or bears financial instruments by any means within the national territory, that he knows or should have presumed that they had illicit origins, with the purpose of avoiding the identification of their origin, their seizure or confiscation; or when a person enters or leaves the country with those goods or just brings or sends those goods by any means, that he knows, or should have presumed that they had illicit origins, with the same purpose above-mentioned.

The money laundering predicates offences included are illegal mining, illicit drug trafficking, terrorism, financing of terrorism, crimes against public administration, kidnapping, procuring, human trafficking, illicit arms trafficking, smuggling of migrants, tax crimes, extortion, robbery, customs offences or any other crime that could generate illicit profits. It is important to note that it is not required to have a conviction on the predicate offence in order to prosecute an individual for money laundering.

Considering the above-mentioned, tax evasion is considered a predicate offence for money laundering.

Finally, is it important to highlight that what must be proven by the prosecutors is that the individual accused of committing money laundering must had known or should have presumed the illicit origin of the assets.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

No. Peruvian law applies only to crimes committed within Peru. Nevertheless, it is possible to investigate money laundering if the predicate offence took place abroad.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Public Prosecutor's Office is the authority responsible for the investigation and prosecution of money laundering crimes. The Financial Intelligence Unit (FIU) is entitled to investigate and analyse financial information in order to determine if there are suspicious activities related to money laundering.

1.5 Is there corporate criminal liability or only liability for natural persons?

The Law N° 30424 regulates corporate liability for various criminal offences, including for money laundering crimes.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Individuals: In the case of aggravating circumstances, money laundering is punishable by a term of imprisonment of between 10 to 20 years, but if the money laundering has its origins from illegal mining, illicit drug trafficking, terrorism, kidnapping, extortion or human trafficking, the term of imprisonment can be up to 25 years. Additionally, a fine is imposed on the individual convicted of money laundering, the amount of the fine varies depending on the individual's wealth.

Legal entities: Money laundering is punishable with a fine that varies depending on the legal entity's income or with another administrative measure. In this sense, if the legal entity's annual income at the time of committing the crime was higher than 1700 UIT (i.e. for 2019, S/. 7 140,000), then the fine could be between 500 UIT (i.e. for 2019, S/. 2 100 000) and 10,000 UIT (i.e. for 2019, S/. 42,000,000). On the other hand, money laundering can also be punished with an administrative measure other than fines; in this case, the maximum penalty can be the dissolution of the legal entity.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is equal to the maximum penalty of the imputed crime. In other words, for simple modalities of money laundering, the statute of limitations would be 15 years, for aggravated circumstances it would be 20 years and if money laundering has its origins from illegal mining, illicit drug trafficking, terrorism, kidnapping, extortion or human trafficking it would be 25 years.

Furthermore, there is an extraordinary statute of limitations, which is equal to the maximum penalty plus its half; this statute of limitations applies since the beginning of the investigations.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes. Enforcement is only at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The Financial Intelligence Unit (FIU) is entitled to order the freezing of assets of those individuals or legal entities that are presumed to be involved in money laundering crimes. The asset freezing order is an exceptional precautionary measure used to forbid the withdrawal, transfer, use, conversion, disposition or movement of funds or other assets of those individuals or legal entities related to money laundering crimes. This measure must be validated or revoked by the judge within a period of 24 hours.

On the other hand, during a criminal procedure, the judge can order a seizure of the goods belonged to the individual that has being accused by the prosecutor. Additionally, there are other procedures (not criminal procedures) which are intended to declare the government as the new owner of goods or assets that have illicit origins.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Until now, no banks nor financial institutions nor their directors, officers or employees have been convicted of money laundering.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

There is an option for individuals who are being investigated or have been condemned for money laundering crimes to reach an agreement with the Public Prosecutor's Office in order to become a special witness or collaborator that will give information related to the crime in exchange for a reduction of the penalty. The records of the fact and terms of such settlements are not public until they are approved by the judge through a sentence.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Anti-money laundering and counter-terrorism financing (AML/CTF) requirements are imposed on financial institutions and other designated businesses by the Financial Intelligence Unit (FIU), following the GAFILAT principles. The most important of such requirements are the following:

- to know your customer (KYC), know your employee (KYE) and, in certain cases, know your vendor or supplier measures;
- to undertake measures to get to know the beneficial owners of an operation, to the extent permitted by due diligence;
- to elaborate bylaws with obligations and measures on AML/CTF that employees must comply;
- to appoint a compliance officer;
- to train employees on AML/CTF topics;
- to undertake a money laundering and terrorism financing risk assessment and monitor such risk on an ongoing basis;
- to take into account the indicators that flag the likelihood of a money laundering or terrorism financing operation in order for the compliance officer to evaluate such operation and, if it is the case, qualify it as a suspicious operation and communicate this to the Financial Intelligence Unit (FIU);
- to maintain a record of certain operations in which the amount of money involved equals or exceeds a threshold determined by the law or, in some cases, by bylaws; and
- to keep copies of documents related to AML/CTF, including customers' and employees' identification documents, for at least 10 years after performing the operations in the case of financial entities and five years in the case of other businesses.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

No. Anti-money laundering requirements imposed to the financial industry only come from the competent authorities.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Compliance and enforcement actions against designated professionals come only from the competent authorities, that is, mainly, the FIU.

2.4 Are there requirements only at national level?

Regulations on anti-money laundering are enforceable throughout the Peruvian territory and therefore the legal requirements regarding anti-money laundering policy are applicable at national level.

Nevertheless, the regulations regarding anti-money laundering take into consideration, especially for the assessment of risks, the places where the operations are performed. For instance, if certain enterprises that should comply with AML/CFT regulations operates or offers its services or products in a place where there is a high rate of money laundering or other similar crimes, then it must apply stricter measures than other enterprises that operate in places where the crime rate is much lower.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

For financial entities, the SBS is the authority in charge of examining and enforcing the anti-money requirements. For other companies that do not have a specific supervisor, the authority in charge is the FIU. If a fine or sanction is applied, the criteria for examination would be publicly available. The FIU's investigations are confidential but the motivation behind a sanction can be checked on the official site of the FIU.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes. The FIU is the competent authority that analyses the information about suspicious clients, workers or suppliers that the financial institutions and other businesses subject to anti-money laundering requirements have to report.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The statute of limitations is four (4) years from the date on which the infraction is committed or since it ceased in the case of a continuous infraction.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

In the case of financial entities, failure to comply with anti-money laundering requirements can be fined with a maximum penalty of 200 UIT (i.e. for 2019, S/. 840,000 or US$ 250,000 approximately). Nevertheless, the administrative authority can apply other types of sanctions, for example, order the company dissolution.

Also, in the case of individuals that are subject to financial regulation (e.g. brokers), failure to comply with anti-money laundering requirements can be fined with a maximum penalty of 100 UIT (i.e. for 2019, S/. 420,000 or US$ 125,400 approximately). Nevertheless, the administrative authority can apply other types of sanctions, for example, cancel the authorisation to operate.

On the other hand, in the case of businesses subject to anti-money laundering requirements, failure to comply with such requirements can be fined with a maximum penalty of 100 UIT (i.e. for 2019, S/. 420,000 or US$ 125,400 approximately). In the case of individuals, failure to comply with anti-money laundering requirements can be fined with a maximum penalty of 15 UIT (i.e. for 2019, S/. 63,000 or US$ 18,805).

In the case of financial entities and individuals subject to financial regulation, the above-mentioned penalties can be applied when they fail to inform the FIU about suspicious operations and when they violate the duty of confidentiality.

In the case of other businesses subject to anti-money laundering requirements, violation of the duty of confidentiality can be fined with the above-mentioned penalties.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Other sanctions are only applied to financial entities and individuals subject to financial regulation, but not to businesses that are only subject to anti-money laundering requirements.

The other sanctions that can be applied are:

- Suspension of operating authorisation.
- Temporary suspension of the inscription in the record managed by the Superintendence of Banking and Insurance (SBS, in Spanish), for a period greater than six and up to 12 months.
- Suspension of the director, manager or any other responsible worker for a period not less than eleven (11) or more than twenty (20) days.
- Cancellation of operating authorisation.
- Exclusion of the inscription in the record managed by the SBS.
- Removal of the director, manager or any other responsible worker, being prevented from re-occupying one of those charges for a period of ten (10) years.
- Disqualification of the director, manager or any other responsible worker for a period of not more than five (5) years.
- Permanent disqualification of the director, manager or any other responsible worker.
- Intervention by the SBS.
- Dissolution and liquidation.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No. Violations of anti-money laundering obligations or requirements are not subject to criminal sanctions. A case for criminal sanction arises when the elements stated in question 1.2 appear.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

Any administrative decision can be appealed at the administrative authority, after which it can be challenged in judicial proceedings. Every process is confidential but the final decision regarding the administrative sanctions is public. Financial institutions are not prone to challenge SBS sanctions in judicial proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The Law 29038 determines the legal entities and individuals that are subject to anti-money laundering requirements ("obliged subjects"):

- All financial and insurance institutions regulated by the Law 26702 (General Law of the Financial and Insurance Systems) and insurance brokers.
- Credit card issuing companies.
- Credit and savings co-operatives.
- Currency Exchange companies.
- Postal Remittance service and/or money order.
- Lending and/or pawning.
- Managers of goods, companies and consortiums.
- Brokerage firms, securities intermediary companies and commodity brokers.
- Mutual funds companies, investment funds and collective investment funds.
- Stock exchange and clearing and settlement institutions.
- Commodity exchange.
- Those who are mainly active in the purchase and sale of vehicles, vessels and aircraft.
- Those who are mainly active in construction activity and/or real estate.
- Real estate agents.
- Those who are mainly active in the activity of casino games and/or slot machines, and/or remote games using the internet or other means of communication.
- Those who are mainly active in the activity of remote sports betting using internet or any other means of communication.
- Those who are mainly active in lottery games and similar.
- Horse racing tracks.
- Customs agents.
- Notaries.
- Mining companies.
- Those who are mainly active in the trade of jewels, metals and precious stones, coins, art objects and postage stamps.
- Laboratories and companies that produce and/or commercialise chemical inputs and controlled goods.
- The companies that distribute, transport and/or commercialise chemical inputs that can be used in illegal mining, under control and supervision of the Peruvian Tax Authority.
- Those who are mainly active in the commercialisation of certain machinery and equipment specified in the National Tariff classification.
- Those who are mainly active in purchase and selling or importation of weapons and ammunition.
- Those who are mainly active in the manufacturing and/or commercialisation of explosive materials.
- Those who are mainly active in crowdlending through virtual platforms.
- Lawyers and public registered accountants that act independently or the law firm or accounting firm that act on behalf or in the interest of their clients with the purpose of (i) performing the purchase and sell of real estate, (ii) managing money and other movable assets, (iii) organising the funding of legal entities, (iv) creating, reorganising or managing legal entities, and (v) performing the purchase or sell of shares.
- Non-profit organisations that raise, transfer and disburse funds, resources or other assets for charitable, religious, cultural, educational, scientific, artistic, social, recreational or solidarity purposes or for the realisation of other types of actions or altruistic or charitable works, when they give credits, microcredits or similar.

The legal entities and individuals that are within the classification above-mentioned, must comply with all the general requirements of anti-money laundering as stated in question 2.1. Nevertheless, the following legal entities and individuals are just obliged to (i) appoint a compliance officer, and (ii) to communicate to the FIU any suspicious operation:

- Those who are mainly active in the commercialisation of antiques.
- Non-profit organisations that raise, transfer and disburse funds, resources or other assets for charitable, religious, cultural, educational, scientific, artistic, social, recreational or solidarity purposes or for the realisation of other types of actions or altruistic or charitable works, when they do not give credits, microcredits or similar.
- Registered lobbyists.
- Public auctioneers.
- Credit and/or debit card processors.
- Travel and tourism agencies and lodging establishments.
- State-owned enterprises other than the ones indicated in the classification above-mentioned, the National Jury of Elections, the National Office of Electoral Processes, the Supervising Agency of the Government Procurement, regional governments and provincial municipalities.
- Peru Compras (public entity, part of the Ministry of Economy and Finance, whose purpose is to optimise public procurement at national level).
- Professional football clubs of the first and second division.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

There is no regulation on the cryptocurrency industry, meaning that companies and individuals that operate with cryptocurrencies (e.g. cryptocurrencies exchanges) are not subject to special requirements, for example, anti-money laundering requirements.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

The Compliance Officers of the financial entities and individuals regulated by the Resolution SBS N° 2660-2015 must elaborate and maintain an annual compliance programme with the methodology for the execution of anti-money laundering-related activities, the dates of execution and the people in charge of each activity.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Obliged subjects must record certain transactions and operations in which the amount of money involved exceeds the threshold

determined by the regulation. The thresholds vary depending on the type of operation (e.g. lending, currency exchange, etc.) and the type of obliged subject (e.g. financial institutions or other businesses). These records must be filed and kept by the obliged subject, available for the competent authorities.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No. There are no requirements other than the recordkeeping of large currency transactions.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes. Reporting requirements apply to the obliged subjects listed in question 3.1 in spite of the origin of the transaction. If it is a cross-border transaction in which the obliged subject is part of and it exceeds the applicable threshold, it must be reported to the competent authority.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Both financial institutions and other businesses subject to anti-money laundering requirements must fulfil three phases of KYC measures:

(i) Identification phase – consists of developing and implementing procedures to obtain the information that allows to determine the identity of a customer or final beneficial owners.

(ii) Verification phase – involves the application of verification procedures at the beginning of the contractual relationship with respect to the information provided by customers and, if so, of its final beneficial owner, in order to ensure that they have been duly identified. If needed, this procedure can be done after the contractual relationship has begun.

(iii) Monitoring phase – intended to ensure that the operations performed by the customers are compatible with what is established in their profile. Also, the monitoring allows to reinforce and reaffirm the knowledge that the companies have about their customers, as well as to obtain more information when they have doubts about the accuracy of the data provided by the customers.

The information that they must obtain from their customers in the identification phase are the following:

Individuals:

- Names and surnames.
- Type of identity document and its number.
- Nationality and residence.
- Home address.
- Telephone number and e-mail address.
- Purpose of the operation to be performed.
- Occupation and profession.
- Indicate if the customer is a Politically Exposed Person (PEP) or has been a PEP, and information related to it.
- Information about the beneficial owner of the operation.

Legal entities:

- Corporate name.
- Taxpayer Identification Number.
- Legal entity main activity.
- Identification of the shareholders that have directly or indirectly more than 25% of the share in the legal entity.
- Purpose of the operation to be performed.
- Identification of the legal representative.
- Address and phone number of the main office.
- In case the customer uses cash, origin of the money involved.

Moreover, in the following cases, the obliged subjects must carry out reinforced KYC measures:

- Customers that are non-resident.
- Legal entities with no address in the Peruvian territory.
- Trusts.
- PEP or a customer that is relative of a PEP or legal entities that have among its shareholders a PEP with equal or more of 25% of the share capital.
- Customers that are being investigated for money laundering or financing of terrorism or predicate offences. Also applies for customers that have any kind of link with people or legal entities that are being investigated for the mentioned crimes.

Additionally, in the specific cases of financial institutions and individuals regulated by the Resolution SBS N° 2660-2015, they also must carry out reinforced KYC measures in the following cases:

- Non-profit organisations, like those entities or legal structures that are mainly engaged in the collection and disbursement of funds for charitable, religious, cultural, educational, social or fraternal purposes or for the realisation of another type of charities or non-profit works.
- Legal entities or individuals that receive transfers of funds from countries that are not cooperating with the Financial Action Task Force (FATF), or that are considered with money laundering and financing of terrorism risks, or with poor banking supervision or countries sanctioned by the Office of Foreign Assets Control – OFAC.
- Dedicated to correspondent services with foreign companies established in countries of low or no taxation, as indicated by the tax authority, or that do not have banking regulation or supervision.

Finally, the reinforced KYC measures that the obliged subjects must apply are the following:

- In the case of PEP, the names of its relatives until the second degree of consanguinity and second of affinity is required, and of the spouse or cohabitant, as well as the relation with legal entities where it maintains a share percentage equal or more than 25% of its share capital, contribution or participation.
- Increase the frequency in the review of the customer's transactional activity.
- Conduct inquiries and apply additional measures of identification and verification, such as: obtaining information about the main suppliers and clients; collecting information from public or open sources; and making home visits.
- To take a decision on beginning or maintaining the relation with the customer. This decision must be taken by the most important manager in the organisation or by another manager or committee designated.

Additionally, in the specific cases of financial institutions and individuals regulated by the Resolution SBS N° 2660-2015, they

must also increase the frequency in the update of the information of the customer and, if it is a legal entity, an annual updating of their shareholders, partners, associates or equivalent title, which have directly or indirectly more than 25% of their share capital, contribution or participation.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

In Peru, financial entities are prohibited to operate with shell banks. Moreover, they must verify that their international counterparts do not operate with shell banks.

3.9 What is the criteria for reporting suspicious activity?

There is no established criteria for identifying and reporting suspicious activities; the criteria used depends on the evaluation of the Compliance Officer. Nevertheless, the term "suspicious activities" is defined by the norms that regulates anti-money laundering as "*Operations carried out or which have been attempted, whose amount or features have no relation to the economic activity of the client or that do not have economic basis; or which by their number, quantities transacted or the particular characteristics of these, may lead reasonably to suspect that the obliged subject is being used to transfer, manage, exploit or invest resources from criminal activities or intended to its funding*". Moreover, the norms contain lists of examples of unusual and suspicious activities that facilitates the evaluation of the Compliance Officer.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes. Firstly, there is a public registry of the Superintendence of Public Registries that maintains information about all legal entities and its shareholders, directors and managers.

Secondly, in the case of financial institutions, the SBS maintains current and adequate information about legal entities and their management and ownership. Moreover, the Financial Intelligence Unit (FIU) also maintains information regarding ownership and management, and other information relevant for anti-money laundering, of the obliged subjects, which includes financial institutions and other businesses. The obliged subjects, depending on if it is a financial institution or other business, have to periodically (quarterly, biannually or annually) report to the FIU about this information.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, as outlined in question 3.6; this also applies for national transactions.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No, it is not permitted.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes. The Resolution SBS N° 789-2018 and the Resolution SBS N° 369-2018 regulate the anti-money laundering requirements for non-financial businesses. The types of businesses subject to anti-money laundering regulation and the requirements have been outlined in questions 3.1 and 2.1. In general terms, non-financial institutions businesses must comply with less anti-money laundering requirements than financial institutions.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Yes. The obliged subjects are listed in question 3.1 and they are required to comply with Law 29038 and its rules.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Recently, in 2018, the Congress of Peru enacted the Legislative Decree N° 1372 that imposes obligations on legal entities to identify and report the personal data of their beneficial owners (i.e. the people who effectively control the legal entity according to various criteria, for example, if he owns at least 10% of the share capital). They have to fill out an affidavit with the information mentioned and give it to the tax authority. These measures have been implemented in accordance with the FATF recommendations on tax evasion and anti-money laundering and combatting the financing of terrorism.

Additionally, the government of Peru enacted the "National Policy against money laundering and the financing of terrorism" in 2017. This national policy is the result of coordinated work between public entities and private companies, which outlines principles, guidelines, objectives and standards for the improvement in the application of measures on anti-money laundering and combatting the financing of terrorism.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The last assessment report published by the Financial Action Task Force on Latin America (GAFILAT) in 2008 within the scope of the "III round of Mutual Evaluations" gave Peru the qualification of "Partially Compliance", given that out of the 49 Recommendations (including the 9 Special Recommendations) published in 2003, 10 were compliant, 14 largely compliant, 24 partially compliant and

just one non-compliant; the results of this evaluation led to an enhanced follow-up. Since then, the government of Peru has enacted more laws in order to adequate the regime on anti-money laundering and combatting the financing of terrorism to the new 40 Recommendations and achieve a better qualification for the "IV round of Mutual Evaluations".

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes. The regime on anti-money laundering and combatting the financing of terrorism has been recently evaluated by GAFILAT. This evaluation process was carried out within the scope of the "IV round of Mutual Evaluations", which began on September 29, 2017 and finished in December 2018. The assessment report has not been published yet.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

For information related to anti-money laundering requirements (including laws, regulations, administrative decrees and guidance) visit the following web page: https://www.sbs.gob.pe/prevencion-de-lavado-activos. The information is only in Spanish.

Should you have any question or doubt, please contact Vodanovic Legal contacto@vodanovic.pe.

Ljubica Vodanovic
Vodanovic Legal
Mariscal la Mar Avenue 550
Office 602
Miraflores
Peru

Tel: +511 326 8948
Email: lvodanovic@vodanovic.pe
URL: www.vodanovic.pe

Ljubica Vodanovic is an expert in Financial Regulation. She graduated with honours from the London School of Economics and holds an LL.M. specialised in Banking and Financial law (2002–2003). She has worked for 11 years (2002–2013) as Executive Coordinator in the Legal Department at the Superintendence of Banking, Insurance and Private Pension Funds (SBS). She was Of Counsel at Philippi, Pietrocarrizosa, Ferrero, DU & Uría (former Delmar Ugarte Lawyers) (2013–2016).

She advises banks, financial and insurance organisations on regulation. Likewise, she also advises local and international companies interested in providing financial services in Peru. Moreover, she is considered one of the leading lawyers in banking and financial regulation in Peru, according to the 2018 and 2019 editions of the ranking *Chambers and Partners*.

In addition, she is in charge of the course 'The Financial System Regulation' at Pontificia Universidad Católica del Perú (PUCP) and Universidad del Pacífico (UP). She has also given presentations in seminars, conferences and workshops on topics related to Banking and Finance Law.

She speaks English and Spanish fluently.

Adolfo Morán
Vodanovic Legal
Mariscal la Mar Avenue 550
Office 602
Miraflores
Peru

Tel: +511 326 8948
Email: amoran@vodanovic.pe
URL: www.vodanovic.pe

Adolfo Moran graduated from the Pontifical Catholic University of Peru (PUCP) Law School in December 2016.

He carried out his career's orientation in Financial Law, Contract Law, Tort Law, Privacy Law and LegalTech. His academic background includes:

- Arbitration litigation techniques training, and he was a member of the team that represented PUCP and won first place of the IX International Championship on Arbitration and Commercial Law held in Madrid, Spain in 2017.
- He is a teaching assistant of "Tort Law" at PUCP Law School.

He speaks Spanish, English and French.

vodanovic legal

We are a legal firm specialised in financial regulation, focused on the use of technology for the provision of financial services. We aim to be the legal support that helps to develop a more efficient and inclusive financial market, that relies on technology to innovate the high standards of regulatory compliance.

The main Peruvian banks and financial institutions, as well as local and international non-regulated companies, come to the firm for legal advice on financial services. Due to the firm's extensive knowledge on financial regulation and the experience of its members who have worked in the Peruvian Supervisor of the financial system (SBS), the firm has an advantage that is unique in the local market. In fact, the lawyers have a particular insight of the financial sector because they know how it works, what concerns arise, what norms apply and how the authorities interpret those norms.

The founding partner Ljubica Vodanovic has been recognised as a leading lawyer in financial regulation by the prestigious *Chambers & Partners* 2018 and 2019 editions.

Philippines

Roberto N. Dio

Castillo Laman Tan Pantaleon & San Jose

Louie Alfred G. Pantoni

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering is a criminal offence under Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001", as amended ("AMLA"). The law created the Anti-Money Laundering Council ("AMLC"), which is the primary government agency tasked with implementing the AMLA and causing the filing of complaints for the prosecution of money laundering offences.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Money laundering is an act, series or combination of acts whereby proceeds of an unlawful activity, whether in cash, property or other assets, are converted, concealed or disguised to make them appear to have originated from legitimate sources. It includes an attempt to transact such assets. Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required under the AMLA to be reported to the AMLC, fails to do so (*AMLA, Sec. 4*).

A "covered person" refers to the following: (a) banks and other institutions regulated by the *Bangko Sentral ng Pilipinas* ("BSP") (*i.e.*, the central bank of the Philippines); (b) insurance companies and other institutions regulated by the Insurance Commission ("IC"); (c) securities dealers and other institutions regulated by the Securities and Exchange Commission ("SEC"); and (d) casinos, among others (*AMLA, Sec. 3(a)*). A "covered transaction" refers to any transaction in cash or other equivalent monetary instrument involving a total amount in excess of PhP500,000 within one business day (*AMLA, Sec. 3(b)*).

In order to establish money laundering, the government must prove the elements of the crime, described above, beyond reasonable doubt. There are two ways by which money laundering can be committed. First is when the proceeds of an unlawful activity are disguised to make it appear that it originated from a legitimate activity. Second is when a covered person fails to report a covered or suspicious transaction. The first refers to a positive act while the second refers to an omission.

Under the AMLA, the term "unlawful activity" includes criminal offences such as kidnapping for ransom, drug offences, plunder, robbery and extortion, swindling, and smuggling, among others (*AMLA, Sec. 3(i)*). Tax evasion is not an offence expressly enumerated as a predicate offence for money laundering.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

No, the AMLA does not have extraterritorial application. The crime of money laundering must be committed within the Philippine territory for it to be punishable under the AMLA.

Money laundering of proceeds of foreign crimes is punishable under the AMLA (*AMLA, Sec. 3(i)(34)*), provided that any element of the money laundering offence is committed within the territory of the Philippines.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The AMLC is the government authority mandated to implement the AMLA. As part of its functions, the AMLC may investigate suspicious transactions and commence civil forfeiture proceedings and all other remedial proceedings through the Office of the Solicitor General ("OSG") (*AMLA, Secs. 7(3) and 7(5)*). The AMLC may impose administrative sanctions and cause the filing of criminal complaints for money laundering with the Department of Justice ("DOJ") or the Ombudsman for the prosecution of money laundering offences (*AMLA, Secs. 7(4) and 7(11)*). The prosecution of money laundering criminal offences is handled by the DOJ, unless they are committed by public officers, in which case they are handled by the Ombudsman.

1.5 Is there corporate criminal liability or only liability for natural persons?

Yes. The AMLA imposes criminal liability not only on natural persons but also on corporations or juridical persons. If the offender is a corporation, association, partnership or any juridical person, its licence can be suspended or revoked by the court upon conviction but the other penalties provided under the AMLA shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed the commission of the crime by their gross negligence (*AMLA, Sec. 14*).

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalties imposable under the AMLA for money laundering offences are imprisonment from six months to 14 years and a fine of not less than PhP3,000,000 but not more than twice the value of the monetary instrument or property involved in the offence (*AMLA, Sec. 14*). The court may also order the freezing, seizure, or forfeiture of the assets subject of a monetary laundering offence, or payment of an amount equal to the value of said assets *in lieu* of forfeiture.

If the offender is a juridical person, the court may also suspend or revoke its licence.

1.7 What is the statute of limitations for money laundering crimes?

As the AMLA does not provide for its own statute of limitations, Act No. 3326, as amended, governing the prescription of offences punished under special laws, shall be applicable. Depending on the act of money laundering committed and its corresponding imposable penalty, the prescription of offences under the AMLA ranges from four to 12 years (*Act No. 3326, as amended, Sec. 1*).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Since AMLA is a national legislation, enforcement is carried out only at the national level. There are no parallel state or provincial criminal offences.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The AMLC is the government authority mandated to institute civil or criminal forfeiture under the AMLA. The AMLC, through the OSG, may file a petition for civil forfeiture of any monetary instrument or property that relates to money laundering. The civil forfeiture may include other monetary instruments or property having an equivalent value to that of the monetary instrument or property found to be related in any way to the money laundering offence, when the actual monetary instrument or property subject of the money laundering cannot be reached by the AMLC (*AMLA, Sec. 12(a)*). More importantly, the petition for civil forfeiture shall proceed independently of the criminal prosecution (*Rule 26, Sec. 2, 2018 Implementing Rules and Regulations ("IRR") of the AMLA; A.M. No. 05-11-04, Sec.28*).

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

To date, the Supreme Court has not decided any case involving a bank or other regulated financial institution or any directors, officers, or employees who were found guilty of the crime of money laundering. As decisions of lower courts are not published, it cannot be confirmed if a bank or other regulated financial institution or any directors, officers, or employees have been convicted of money laundering. In early 2019, it was reported in local news that a lower court convicted a branch manager of a major local commercial bank of money laundering in a cyberheist involving US$81 million stolen from Bangladesh Bank's account with the Federal Reserve Bank of New York in February 2016. The bank manager was sentenced to imprisonment of four to seven years for each of the eight counts of money laundering for which she was convicted and fined US$109.5 million.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Under Philippine law, criminal actions cannot be settled outside of the judicial process. However, the civil aspect of these criminal actions may be the subject of a settlement. Records of the fact and terms of settlements are not made public.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The AMLA, its IRR, the AMLC Regulatory Issuance (B) No. 1 (2018) known as the "Anti-Money Laundering/Counter-Terrorism Financing Guidelines for Designated Non-Financial Businesses and Professions", the AMLC Registration and Reporting Guidelines ("AMLC Guidelines"), and Republic Act 10168, otherwise known as "The Terrorism Financing Prevention and Suppression Act of 2012" ("RA 10168") impose anti-money laundering obligations on financial institutions and other covered persons.

These include:

- a report to the AMLC of all "covered transactions" (for casinos, a single casino cash transaction involving an amount in excess of PhP5,000,000 or its equivalent in any other currency), and all "suspicious transactions" – regardless of the amount involved – within five working days of its occurrence;
- prohibition of anonymous accounts, accounts under fictitious names, numbered accounts and similar accounts;
- keeping records of all transactions for five years from date of occurrence;
- conducting a Know-Your-Customer ("KYC") procedure or customer due diligence based on a risk-based approach;
- developing clear, written and graduated customer acceptance policies and procedures, including a set of criteria for customers that are likely to post low, normal or high-risk operations;
- observing ongoing monitoring of customers, accounts and transactions;
- registering with AMLC's electronic reporting system and updating the registration every two years;
- recording the identity of immediate family members and entities related to politically-exposed persons;
- giving to the AMLC full access to all information pertaining to a transaction upon receipt of a bank inquiry order;
- providing training for officers and personnel;

- keeping reports confidential and prevent tipping-off;
- putting systems in place that alert its responsible officers of any suspicious money laundering, activity or transaction, and developing its own list of alerts or red flags;
- formulating an internal reporting chain;
- developing a written Money Laundering/Terrorist Financing Prevention Program ("MTPP");
- identifying and verifying beneficial owners;
- uploading KYC documents, if the reason for suspicion is a predicate crime;
- for casinos, to: conform to high ethical standards and observe good corporate governance; and
- designate a compliance officer; and conduct independent internal audit examinations at least once every two years.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes. The Capital Markets Integrity Corporation ("CMIC") of the Philippine Stock Exchange ("PSE") has adopted its own set of rules and regulations implementing the AMLA as a guide to trading participants.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, in some cases. For example, the CMIC monitors compliance and imposes sanctions on PSE trading participants who violate the AMLA.

2.4 Are there requirements only at national level?

Yes, the requirements are imposed at national level only.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The AMLC and the Anti-Terrorism Council ("ATC") of the BSP are responsible for monitoring compliance with and enforcement of anti-money laundering requirements.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes. The AMLC functions as both the FIU and regulator of anti-money laundering laws in the Philippines.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The AMLA does not provide a specific statute of limitations for bringing administrative and civil forfeiture cases. However, under the Civil Code of the Philippines, the statute of limitations for civil actions arising from an obligation created by law is 10 years (*Civil Code, Art. 1144(2)*). For the statute of limitations for prosecution of money laundering criminal offences, see question 1.7 above.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Administrative fines shall be in amounts determined by the AMLC to be appropriate, which shall not be more than PhP500,000 per violation (*IRR, Rule 26*).

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The imposition of fines may be dispensed with in case of light violations, where the violators may receive warning or reprimand if corrective action was immediately taken after the covered entity's attention was called by the AMLC. For a less serious violation, a warning may suffice for a first-time violation where corrective action was immediately taken. For a serious violation, a fine will not be imposed for a first offence if prompt corrective action is immediately carried out and no aggravating circumstance is present.

Upon a finding of probable cause, an *ex parte* petition for forfeiture may be commenced as well as an *ex parte* petition for the issuance of a six-month freeze order of any monetary instrument or property alleged to be laundered, its proceeds, and the instrumentalities used in furtherance of the unlawful activities (*AMLA, Secs. 10 and 12*).

Public officials or employees found guilty of violations may suffer perpetual or temporary absolute disqualification from office.

Banks and other regulated financial institutions may impose sanctions by way of financial exclusion, such as by denying services or by suspending or closing accounts.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Penalties are not only administrative or civil in nature. Violations of anti-money laundering obligations are also subject to criminal sanctions (*AMLA, Sec. 14*).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

In the exercise of its compliance review functions, the AMLC issues a Report of Compliance or a Report of Examination that may serve as basis for a formal charge after the conduct of a preliminary administrative investigation. After receipt of the alleged violator's answer, a clarificatory meeting may be held. The administrative proceedings shall end upon the issuance of the Resolution by the AMLA. A motion for reconsideration may be filed upon any ground allowed by law. Collection may be enforced by issuance of a Notice of Execution by the AMLC.

Administrative proceedings are confidential and may only be inquired into by the parties involved. Decisions of the AMLC may be challenged before the Court of Appeals, and ultimately before the Supreme Court of the Philippines.

Financial institutions have not challenged penalty assessments, but account holders have successfully challenged the AMLC's applications for bank inquiries and freeze orders in judicial proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The following financial institutions are covered by the AMLA and subject to anti-money laundering requirements:

- banks and all other similar institutions supervised or regulated by the BSP;
- insurance companies and all other institutions supervised or regulated by the IC; and
- securities dealers and other entities administering or otherwise dealing in currency or other similar monetary instruments or property supervised or regulated by the SEC.

Other designated non-financial businesses and professions are also subject to anti-money laundering requirements (*AMLA, Secs. 3(a)(4) to 3(a)(7)*).

Casinos, including internet- and ship-based casinos operating within the Philippine territory, with respect to their casino cash transactions related to their gaming operations, are also required to comply with anti-money laundering requirements.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Since an entity that provides virtual currency or cryptocurrency exchange service in the Philippines is required to obtain a certificate of registration to operate as a remittance and transfer company from the BSP and as such is regulated by the BSP, providers of virtual currency or cryptocurrency exchange service in the Philippines may be considered covered by the AMLA (*Manual of Regulations for Non-Bank Financial Institutions, Sec. 4512N.3*).

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes. Covered persons are mandated to maintain a written, comprehensive and risk-based MTPP that are compliant with the AMLA and RA 1068, their IRRs, and other AMLC issuances, and the AML/CTF guidelines of Supervising Authorities ("SAs") and commensurate to their size and risk profile. The MTPP shall include, at the minimum, internal policies, controls and procedures on: (a) risk management; (b) compliance management set-up; (c) screening procedure to ensure high standards when hiring employees; (d) continuing education and training programmes; (e) independent audit functions; (f) details of implementation of customer due diligence; (g) compliance with orders and directives of the AMLC; (h) adequate safeguards on the confidentiality and use of information exchange; and (i) cooperation with the AMLC and SAs (*IRR, Rule 16, Sec. 1*).

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Under the IRR and the AMLC Guidelines, all records of all transactions of covered institutions shall be maintained and safely stored for five years from the dates of the transactions. Closed accounts shall be preserved and safely stored for at least five years from the dates when they were closed.

Covered institutions shall report covered transactions to the AMLC within five working days from occurrence. The institutions and their officers, employees, representatives, agents, advisors, consultants, or associates shall not directly or indirectly communicate to any person the fact that a covered transaction report was made, its contents, or any related information.

A "covered transaction" is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of PhP500,000 within one banking day, a transaction involving previous metals or stones in cash or other monetary equivalent exceeding PhP1,000,000, and for casinos, a covered transaction is a single casino cash transaction involving an amount in excess of PhP5,000,000 or its equivalent in any other currency (*IRR, Rule 2, Sec. 1(w)*).

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

The AMLA, the IRR, and AMLC Guidelines also require the reporting of suspicious transactions (see discussion in question 3.9 below). Rule 22 of the IRR states that covered persons shall ensure the accuracy and completeness of covered transaction reports and suspicious transaction reports, which shall be filed in the AMLC-prescribed forms and shall be submitted in electronic form and in a secured manner to the AMLC.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes. Under Rule 19 of the IRR, covered persons are required to:

- gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of its supervision, including whether it has been subject to a money laundering and terrorist financing ("ML/TF") investigation or regulatory action;
- assess the respondent institution's anti-money laundering and combatting the financing of terrorism ("AML/CFT") controls;
- obtain approval from senior management before establishing new correspondent relationships; and
- clearly understand the respective AML/CFT responsibilities of each institution.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Under Rule 18 of the IRR, covered persons shall establish and record the true identity of their clients based on official documents and shall maintain a system of verifying their identity. In case of

corporate clients, they shall maintain a system of verifying their legal existence, organisational structure, and authority and identification of all persons purporting to act on their behalf. Anonymous accounts, accounts with fictitious names, and all other similar accounts are absolutely prohibited.

Further, in conducting customer due diligence, a risk-based approach shall be undertaken depending on the type of customer, business relationship, or the nature of the product, transaction or activity.

In customer identification, covered persons shall conduct face-to-face contact or as reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business, and the risks involved; provided that money laundering risks are effectively managed.

Where lower risks of money laundering and terrorist financing have been identified, through an adequate analysis of risk by the covered persons, reduced due diligence procedures may be applied. On the other hand, where risks of money laundering or terrorist financing are higher, covered persons shall be required to conduct enhanced due diligence measures, consistent with the risks identified. This shall require gathering additional customer information and identification documents, among others.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes. No shell bank is allowed to operate or be established in the Philippines. Covered persons shall not enter into, or continue, correspondent banking relationships with shell banks and shall have measures to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks (*IRR, Rule 19, Sec. 3.5*). Covered institutions shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks (*IRR, Rule 19, Sec. 7.2*).

3.9 What is the criteria for reporting suspicious activity?

Transactions, regardless of the amount involved, are considered suspicious activity when any of the following circumstances exist:

- there is no underlying legal or trade obligation, purpose or economic justification;
- the client is not properly identified;
- the amount involved is not commensurate with the business or financial capacity of the client;
- taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
- any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
- transaction is in any way related to money laundering/terrorism financing or related unlawful activity that is about to be, is being, or has been committed; and
- any transaction that is similar, analogous, or identical to any of the above.

Covered persons shall report to the AMLC all covered transactions and suspicious transactions within five working days from its occurrence, unless the supervision authority prescribes a longer period not exceeding 10 working days (15 working days, in case of casinos). If a transaction is both a covered transaction and a suspicious transaction, it shall be reported as a suspicious transaction.

When reporting suspicious transactions to the AMLC, covered persons, their officers, and employees are prohibited from directly or indirectly disclosing the fact that a suspicious transaction report has been or is about to be reported, its contents, or any other related information. Any such information shall not be published or aired, in any manner or form, by the mass media, or through electronic mail, or other similar devices (*IRR, Rule 22, Sec. 6.2*).

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes. The BSP, SEC, and IC maintain current and adequate information about the management and ownership, of legal entities that are under their supervision and jurisdiction, including the company directors, shareholders, and their corresponding holdings. New SEC regulations on disclosure of beneficial ownership of corporations and partnerships is expected to take effect on June 30, 2019.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes. Covered persons shall establish policies and procedures designed to prevent wire/fund transfers from being utilised for money laundering activities. Financial institutions shall not accept instructions for wire transfer from a non-customer originator, for occasional transactions exceeding the set threshold, unless it has conducted the necessary customer due diligence measures to establish the true and full identity and existence of said originator (*IRR, Rule 19, Sec. 6.1.1*).

Financial institutions shall ensure that all cross-border wire transfers in the amount or threshold to be determined by the BSP or its equivalent in foreign currency are always accompanied by: (a) required and accurate originator information, such as name, account number or transaction reference number, and originator's address, or national identity number, or customer identification number, or date and place of birth; and (b) required beneficiary information, such as name and account number or transaction reference number (*IRR, Rule 19, Sec. 6.1.2*). The same requirements apply to *de minimis* thresholds set by the BSP (*IRR, Rule 19, Sec. 6.1.4*).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No. Ownership of legal entities established in the Philippines, in the form of bearer shares, is not permitted. However, covered persons may deal with bearer share entities established in foreign jurisdictions. A covered person dealing with bearer share entities established in foreign jurisdictions shall conduct enhanced due diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account (*IRR, Rule*

19, Sec. 7). These entities shall be subject to ongoing monitoring at all times, and the list of stockholders and/or beneficial owners shall be updated within 30 days after every transfer of ownership. The appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

None. The requirements stated in questions 3.4 and 3.9 are applicable to all covered persons, including non-financial institution businesses.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Yes. Aside from the general requirements under the IRR, Section 13 of the Casino Implementing Rules and Regulations ("CIRR") of Republic Act No. 10927 requires casinos to designate a compliance officer of senior management status, with the authority and mandate to ensure day-to-day compliance with its AML/CFT obligations. Further, if a casino's activities are complex or if it maintains multiple business locations, it shall decide if it is necessary to create a compliance office or to appoint a compliance officer for each of the casino's locations. The casino shall also designate a separate officer to be responsible and accountable for all record-keeping requirements. The compliance and record officers shall be responsible for making the records readily available to the AMLC upon request.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

There is a pending Senate Bill No. 1256 ("SBN 1256"), which seeks to further strengthen and amend the AMLA. Some of the proposed amendments are:

- expansion of the list of covered persons to include money service business, trust companies, and real estate developers, among others;
- adding more unlawful activities (this term is proposed to be replaced with "Predicate Offense");
- adding provisions on retention of forfeited assets and cross-border declaration; and
- repealing the provision on non-intervention in the operations of the Bureau of Internal Revenue.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The FATF has recognised the significant improvement in the AML/CFT regime of the Philippines. The Philippines is no longer subject to FATF monitoring under its global AML/CFT compliance process. The main concern raised in the Mutual Evaluation Report in 2009 in relation to casinos was addressed by the enactment of new legislations on this matter.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes. A Mutual Evaluation of the Philippines's AML/CTF regime was conducted in 2009 by the World Bank and was discussed and adopted by the plenary of the Asia/Pacific Group ("APG") on Money Laundering. A copy of the report is available on APG's website. A Mutual Evaluation of the Philippines's AML/CTF regime was conducted in 2009 by the World Bank and was discussed and adopted by the plenary of the Asia/Pacific Group ("APG") on Money Laundering. A copy of the report is available in APG's website http://www.apgml.org/documents/search-results.aspx?keywords=philippines.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The official website of AMLC, www.amlc.gov.ph, provides information on the relevant anti-money laundering laws, regulations, issuances, and pending legislation. The materials are publicly available in English.

Roberto N. Dio

Castillo Laman Tan Pantaleon & San Jose
3/F, 122 The Valero Tower
Valero Street, Salcedo Village
Makati City 1227
Metro Manila
Philippines

Tel: +632 817 6791 to 95
Email: RND@clptsj.com.ph
URL: www.cltpsj.com.ph

Roberto N. Dio is recognised as a leading practitioner in litigation and dispute resolution in the Philippines. He has advised various clients on complex issues involving bankruptcy and insolvency, bank closures and regulations, debt recovery and foreclosure, government contracts, commercial and property disputes, unfair competition, insurance, and maritime cargo claims. He has acted as counsel in civil, criminal and administrative litigation and has successfully handled several cases before the Supreme Court, including the dismissal of a mass tort damage suit related to a nematocide applied in banana farms and the dismissal a petition to stop the construction of a high-rise condominium behind a national monument.

He is an active commercial and construction arbitrator and currently serves as the secretary general of the Philippine Dispute Resolution Center, the country's leading ADR institution. He has practised for more than 30 years and served in several capacities in the management of the firm, including as head of its litigation practice group. He has written numerous legal articles and is a volunteer lawyer at the University of the Philippines Office of Legal Aid.

Louie Alfred G. Pantoni

Castillo Laman Tan Pantaleon & San Jose
5/F, 122 The Valero Tower
Valero Street, Salcedo Village
Makati City 1227
Metro Manila
Philippines

Tel: +632 817 6791 to 95
Email: LGP@cltpsj.com.ph
URL: www.cltpsj.com.ph

Louie Alfred G. Pantoni is a Partner at Castillo Laman Tan Pantaleon & San Jose. His expertise includes corporate and project finance, foreign investments, energy, banking, securities, mergers and acquisitions, pharmaceutical law, corporate law, data privacy, competition law and intellectual property. He has worked on various mergers and acquisitions and financing transactions involving local and foreign clients. He has assisted investors, international financial institutions and banks in their investments in renewable and non-renewable energy, pharmaceuticals, advertising and online platforms, real estate development and infrastructures in the Philippines. For a time, he was seconded to a multilateral financial institution to handle equity and debt transactions.

He has also counselled various clients on anti-bribery and anti-money laundering laws. He likewise regularly reviews contracts and policies for clients with anti-money laundering aspects and clauses.

CASTILLO LAMAN TAN
PANTALEON & SAN JOSE
LAWFIRM

Castillo Laman Tan Pantaleon & San Jose advises local and international clients in all aspects of Philippine law. The firm excels in both advisory and implementation work, provides efficient, value-added legal service and assists multi-sectoral clients in understanding Philippine law and implementing their objectives. The synergy of legal professionals of various expertise has equipped the firm with organised capability to handle cases and projects of varying magnitude and nature. The core competencies of the firm include business counselling and protection of client's rights in any given legal situation. It is one of the most active transaction lawyers handling the Philippine phase of many worldwide mergers, acquisitions and other forms of corporate reorganisations. The firm also has strong litigation group with extensive experience and handles civil, commercial, criminal, tax and specialised litigations before judicial and quasi-judicial bodies.

Poland

Wojciech Kapica

Zuzanna Piotrowska

SMM Legal Maciak Mataczyński Adwokaci Sp.k.

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In Poland, money laundering is prosecuted by public prosecutor's offices. Regional Prosecutor's Offices conduct and supervise the penal proceedings in criminal cases connected with the most serious criminal, financial and tax offences. Investigations are conducted either by public prosecutors or by the local police.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Article 299 of the Polish Criminal Code states that anyone who receives, transfers or transports abroad, or assists in the transfer of title or possession of legal tender, securities or other foreign currency values, property rights or real or movable property obtained from the profits of offences committed by other people, or takes any other action that may prevent or significantly hinder the determination of their criminal origin or place of location, their detection or forfeiture, is liable to imprisonment of between six months to eight years. Besides that, anyone who as an employee of a bank, financial or credit institution, or any other entity legally obliged to register transactions and the people performing them, unlawfully receives a cash amount of money or foreign currency, or who transfers or converts it, or receives it under other circumstances raising a justified suspicion as to its origin from the offences specified above, or who provides services aimed at concealing its criminal origin or in securing it against forfeiture, is liable to the penalty specified above. If the offender commits an act specified above acting in concert with other people, he or she is liable to imprisonment of between one to 10 years.

Tax evasion is not a predicate offence for money laundering. Tax evasion is an offence according to the Polish Penal Fiscal Code.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In principle, according to article 5 of the Polish Criminal Code, Polish criminal law applies to an offender who commits a prohibited act in the Republic of Poland, or on a Polish vessel or aircraft, unless the Republic of Poland is a party to an international agreement stating otherwise.

In addition, the Polish Criminal Code applies also to Polish citizens who have committed an offence abroad (article 109 of the Polish Criminal Code) as well as to foreigners who have committed a prohibited act abroad that is against the interest of the Republic of Poland, a Polish citizen, a Polish legal entity or a Polish organisational unit without the status of a legal entity. Besides that, Polish criminal law applies to foreigners who have committed a prohibited act abroad other than acts mentioned above, if, under Polish criminal law, the prohibited act is subject to a penalty exceeding two years' imprisonment, where the offender is in the Republic of Poland and where no decision on his or her extradition has been taken.

For an act committed abroad to be considered an offence, it must be considered an offence by the law in force where it was committed (article 111 § 1 of the Polish Criminal Code).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Public prosecutor's offices are responsible for this.

1.5 Is there corporate criminal liability or only liability for natural persons?

Polish criminal law applies only to natural persons. However, the so-called collective entities bear liability for acts prohibited under penalty as offences or fiscal offences according to rules stated in the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited Under Penalty (hereinafter referred to as "the Act").

Pursuant to article 2 of the Act, a collective entity is a legal person and organisational unit without legal personality on which separate laws and regulations confer legal capacity, except for the State Treasury, local governments units and their unions. A collective entity according to the Act is also a commercial company with the shareholding of the State Treasury as well as a company with the shareholding of local governments units or union of such units, a company in organisation, an entity in liquidation and an entrepreneur not being a natural person and foreign organisational unit.

According to the Act, a collective entity may hold responsibility for, *inter alia*, all offences related to economic activity, penal and fiscal offences, public corruption and corruption in business, including the crime of money laundering.

A collective entity bears liability for the prohibited act committed by a natural person if such behaviour brought or might have brought to collective entity some benefit (even immaterial). A collective entity bears such liability if the person:

- acts on behalf or in the interest of the collective entity within the scope of power or duty to represent it, makes decisions on its behalf or exercises internal control, or in having exceeded such power or failed to perform this duty;
  - was permitted to act, as a result of having exceeded powers or failed to perform the duties by the person referred to in above; and
  - acts on behalf or in the interest of the collective entity, with the consent or knowledge of the person referred to above.

According to article 4 of the Act, the collective entity bears liability if the fact of committing the prohibited act by the person mentioned above has been approved by a valid judgment convicting such person, a decision on conditional discontinuance of penal proceedings or proceedings in the case involving a fiscal offence in respect of such person or if a decision permitting such person to voluntarily accept the liability or a court decision on discontinuance of proceeding against such person due to a circumstance excluding the punishment of the perpetrator.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Money laundering is punishable by imprisonment of between six months to eight years. However, if the offender commits the act of money laundering acting in concert with other people as well as in the case where offender gains significant material benefit, he or she is liable to imprisonment of between one to 10 years.

In reference to collective entities, the court adjudicates a monetary penalty in the amount of PLN 1,000,000 to 5,000,000 not exceeding, however, 3 per cent of the revenue earned in the financial year in which the prohibited act forming the grounds for liability of the collective entity was committed.

In respect of collective entities, the court should also decide the forfeiture of the following:

- objects coming, even indirectly, from the prohibited act or objects which served or were designed for committing the prohibited act;
- material benefit coming, even indirectly, from the prohibited act; and
- the value equivalent to the value of objects or material benefits coming, even indirectly, from the prohibited act.

Apart from what is stated above, the following may be adjudicated in respect of collective entities:

- prohibition of promotion or advertising of the conducted activity, manufactured or sold products and provided services or performances;
- prohibition of benefiting from grants, subventions or other forms of financial support involving public funds;
- prohibition of benefiting from assistance of international organisations of which the Republic of Poland is a member;
- prohibition of bidding for public contracts;
- repeals; and
- making the judgment publicly known.

The abovementioned prohibitions are adjudicated for a period of between one year and five years.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations for money laundering is 15 years from the moment the offence was committed (article 101 § 1 point 2a of the Polish Criminal Code).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

There are no parallel state or provincial criminal offences in Poland.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

According to the Polish Criminal Code, in the case of criminal conviction for money laundering, the court orders the forfeiture of items derived either directly or indirectly from the offence, or the gains of the offence, or an equivalent value, even if they are not the property of the offender. Forfeiture is not ordered if all or part of the gains, or their equivalent, are returned to the aggrieved party or another entity.

The Polish Criminal Code provides for the possibility of forfeiture if there is no criminal conviction. Pursuant to article 45a of the Polish Criminal Code, the court may order the forfeiture in the case where the effects of a prohibited act on society are insignificant as well as in the case where the court conditionally discontinued criminal proceedings or if the offender has committed a prohibited act in a state of unaccountability or if there are circumstances excluding punishment.

Apart from the above, if evidence collected during proceedings show that in the case of conviction, the forfeiture would be ordered, the court may also order forfeiture in the following situations:

- in the event of the death of the offender;
- in the event of discontinuation of criminal proceedings because of failure to identify the offender;
- in the event of suspension of criminal proceedings; or
- if the accused cannot take part in the proceeding because of mental disorder or other dread disease.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

There are no widely known cases of banks or other financial institutions or their directors, officers or employees to be convicted of money laundering in Poland. However, such cases may have taken place.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

According to Polish Code of Criminal Procedure, there is a possibility to refrain further actions if the accused pleads guilty and in the view of his or her explanations the circumstances of the offence and the guilt of the accused do not raise doubts and the

attitude of the accused indicated the purposes of the proceedings will be achieved. In such case, the public prosecutor, instead of indictment, files with the court a motion to issue a sentence of conviction and imposition on the accused of a penalty or a penal measure agreed with him or her, applicable to summary offence, with which the accused is charged. Arrangements conducted between the public prosecutor and the accused should be reflected in the abovementioned motion.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The following authorities of government administration are competent for the matters of anti-money laundering and terrorist financing:

1) the minister competent for public finance as supreme financial authority; and
2) the General Inspector of Financial Information (Polish Financial Intelligence Analysis Unit).

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

There are no money laundering requirements imposed by self-regulatory organisations or professional associations. Lawyers, notaries and tax advisers are obliged to respect the requirements imposed by the Act of 1 March 2018 on Counteracting Money Laundering and the Financing of Terrorism (hereinafter referred to as "Polish Act on Anti-Money Laundering").

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

No, the authorities listed above in question 2.1 are competent for anti-money laundering compliance and enforcement against members of self-regulatory organisations and professional associations in the scope of Polish Act on Anti-Money Laundering.

2.4 Are there requirements only at national level?

Money laundering requirements are codified in the Polish Act on Anti-Money Laundering. Apart from that, Poland as a member of the European Union, should also respect European regulations and guidelines in this matter.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

The General Inspector of Financial Information is responsible for examination for compliance and enforcement of anti-money laundering requirements. According to the Polish Act on Anti-Money Laundering, the General Inspector of Financial Information in the scope of his tasks, is taking activities with a view to counteracting money laundering and terrorist financing, in particular the General Inspector of Financial Information is, *inter alia*, exercising control over the compliance with the provisions on counteracting money laundering and terrorist financing, handing over to the entitled authorities the information and documents substantiating the suspicion of committing an offence, as well as conducting the procedure of suspension of a transaction or blocking an account and demanding the provision of information on the transaction and making them publicly available.

Additionally, as part of the exercised supervision or conducted inspection, the inspection is also conducted by:

- the President of the National Bank of Poland – with regard to the entities carrying out exchange bureau activity;
- the Polish Financial Supervision Authority – with regard to obliged institutions supervised by the Authority;
- the National Cooperative Savings and Credit Fund – with regard to cooperative savings and credit funds;
- presidents of courts of appeal – with regard to notaries;
- heads of customs and revenue offices – with regard to the obliged institutions supervised by those authorities;
- province governors and district heads – with regard to associations; and
- ministers and district heads – with regard to foundations.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

In Poland, the General Inspector of Financial Information as FIU is, *inter alia*, analysing information on property values which the General Inspector of Financial Information suspects are linked with an offence of money laundering or terrorist financing.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

With regard to money laundering, competent authorities according to the Polish Act of Administrative Proceeding cannot impose an administrative monetary penalty, if a period of five years has elapsed since the infringement of law or occurrence of the effects thereof. Besides that, the administrative monetary penalty is not subject to enforcement after five years since the day when the sanction should have been enforced has passed.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

In principle, the monetary penalty for failure to comply with the regulatory/administrative anti-money laundering requirements may be imposed up to twice the amount of the profit gained or loss avoided by an obligation institution as a result of a violation or – where determining the amount of this profit or loss is not possible – up to the amount of the equivalent of EUR 1,000,000.

Additionally, the monetary penalty against, *inter alia*, banks, investments firms or foreign legal persons carrying out brokerage activity on the territory of Poland, may be imposed up to PLN

20,868,500 in the case of natural persons and up to the amount of equivalent of EUR 5,000,000 or up to the amount of 10 per cent of the turnover shown in the last approved financial statements for a financial year or in the last covered by consolidated financial statements for a financial year in the case of a legal person or an organisational unit having no legal personality.

There are various failures that are subject to the penalty provisions such as:

- failure to discharge the obligation of appointment of a person responsible for the fulfilment of the obligations laid down in the Polish Act on Anti-Money Laundering;
- failure to discharge the obligation of ensuring that the transfer of funds is accompanied by the information on the payer or the recipient;
- failure to discharge the obligation of implementing effective procedures that enable to detect the missing information on the payer or the recipient;
- failure to discharge the obligation of freezing funds or economic resources or the prohibition of making the funds or economic resources available; and/or
- failure to discharge the obligation of application specific restrictive measures.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Besides monetary penalties, the following penalties may be imposed on obliged institutions:

- the publication of the information about an obliged institution and the extent of violation of the provisions of the Polish Act on Anti-Money Laundering by this institution in the official publication on a dedicated website of the office providing support for the minister competent for public finance (pol. *Biuletyn Informacji Publicznej*);
- the order to cease to undertake specific acts by an obliged institution;
- withdrawal of a concession or permission or removal from the register of regulated activity; and
- the prohibition of discharging duties at an executive post by the person liable for the obliged institution's violation of the provisions of the Polish Act on Anti-Money Laundering, for a period not exceeding a year.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, there are also criminal sanctions for violation of anti-money laundering obligations. The following violations are subject to criminal sanction according to article 156 of the Polish Act on Anti-Money Laundering:

- failure to discharge the obligation of providing to the General Inspector of Financial Information the notification about the circumstances that may imply a suspicion of commission of the offence of money laundering or terrorist financing or the obligation of providing to the General Inspector of Financial Information the notification of the arising of a substantiated suspicion that a specific transaction or property values being the subject of this transaction could be linked to money laundering or terrorism financing;
- providing or concealing to the General Inspector of Financial Information inaccurate data concerning transaction, amounts or persons; and
- disclosing to unauthorised persons, account holders or the persons to whom a transaction refers, the information gathered pursuant to the Polish Act on Anti-Money Laundering or making use of this information at variance with the provisions of the Polish Act on Anti-Money Laundering.

In the abovementioned case, the person who commits the act is liable to imprisonment of between three months to five years.

The Polish Act on Anti-Money Laundering also penalises with the fine thwarting or hindering the conduct of the inspection (article 157 of Polish Act on Anti-Money Laundering).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process for assessment and collection of sanctions and appeal of administrative decision is as follows:

Firstly, the competent authority (the General Inspector of Financial Information, the President of the National Bank of Poland or the Polish Financial Supervision Authority), issues a decision.

In the case where the decision was issued by the General Inspector of Financial Information, the obliged institution may submit a complaint to the Provincial Administrative Court within 30 days since the delivery of the decision.

In the case the decision was issued by the President of the National Bank of Poland, the obliged institution may submit a motion for reconsideration. After exhaustion of the abovementioned remedies, the obliged institution may submit a complaint to the Provincial Administrative Court within 30 days since the delivery of the decision. The same procedure applies to the decisions issued by the Polish Financial Supervision Authority.

The General Inspector of Financial Information post the information on a dedicated website of the office providing support for the minister competent for public finance (pol. *Biuletyn Informacji Publicznej*), regarding:

- the issuance of the final decision on imposing of an administrative penalty;
- the lodging of a complaint against such decision; and
- the decision taken as a result of examining the abovementioned complaint.

Such information includes identification data of obliged institutions on which the administrative penalty was imposed, the type and nature of violation of the provisions as well as the type of amount of the imposed administrative penalty.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The Polish Act on Anti-Money Laundering applies to the following entities acting in the course of business in Poland:

- banks and other financial institutions;

- foreign legal persons conducting brokerage activity within the territory of the Republic of Poland, including those conducting such activity in a form of a branch, and commodity brokerage houses;
- companies operating a regulated market-within the scope of the operation of the auction platform;
- insurance undertakings in selected cases and insurance intermediaries;
- Krajowy Depozyt Papierów Wartościowych S.A. and a company to which Krajowy Depozyt Papierów Wartościowych S.A. has delegated activities;
- entrepreneurs conducting exchange office activity and other entrepreneurs providing a foreign exchange service or a foreign exchange intermediation service;
- entities conducting economic activity consisting of providing services in the area of exchange between virtual currencies and means of payment, intermediation in the exchange referred, the operation of the accounts referred in this regard;
- notaries, attorneys, legal counsels, foreign lawyers and tax advisors in certain cases;
- entrepreneurs in certain cases;
- entities conducting activity in the area of the provision of bookkeeping services;
- real estate agents;
- postal operators;
- entities conducting activity in the area of games of chance, betting, card games, and machine games;
- foundations and associations in selected cases; and
- lending institutions.

The Polish Act on Anti-Money Laundering requires obliged institutions to identify and assess the risks associated with money laundering and terrorism financing, implement and apply the financial security measures proportional to the risk identified during customer analysis, gather and transfer to the appropriate institutions information provided for by law, conduct trainings, cooperate with the General Inspector of Financial Information in the event of suspicion of money laundering or financing of terrorism and implement the organisational activities aimed at ensuring proper implementation of basic tasks of obliged institutions.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The institutions that have been added to the catalogue of obliged institutions are the entities conducting economic activity consisting of providing services in the area of exchange between virtual currencies and means of payment, exchange between virtual currencies, intermediation in the exchange and the operation of the accounts. The definition of virtual currencies was introduced.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All obliged institutions are required to implement an internal anti-money laundering and terrorist financing procedure, which must contain the elements indicated in article 50 sec. 2 Polish Act on Anti-Money Laundering. These include:

1) activities or actions taken in order to mitigate any money laundering and terrorist financing risks and to manage appropriately the money laundering or terrorist financing risks identified;
2) rules for identifying and assessing money laundering and terrorist financing risks involved in a given business relationship or occasional transaction;
3) measures applied to manage appropriately the identified money laundering or terrorist financing risk involved in a given business relationship or occasional transaction; and
4) the rules for fulfilling obligations including the provision of information on transactions and notifications to the General Inspector of Financial Information.

Furthermore, in the procedures set out above are also rules for the reporting of actual or potential breaches of provisions on counteracting money laundering and terrorist financing by employees. This is an additional measure to ensure compliance with the law. The abovementioned measures are to ensure obligations are complied with the AML.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

The Polish Act on Anti-Money Laundering does not distinguish specific requirements for recordkeeping or reporting large currency transactions. In this respect, general requirements are applied.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Apart from as stated in question 3.6 below, transactions should be reported when received or a cash payment is made in an amount exceeding the equivalent of EUR 15,000.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

In accordance with article 72 sec. 2 Polish Act on Anti-Money Laundering, the obliged institutions (with exceptions) shall provide the General Inspector with information on an executed transfer of funds for an amount exceeding the equivalent of EUR 15,000, except for:

1) a transfer of funds between a payment account and a term deposit account that belong to the same customer in the same obliged institution;
2) a domestic transfer of funds from another obliged institution;
3) a transaction related to the obliged institution's own operations, carried out by the obliged institution in its own name and on its own behalf, including a transaction concluded on the interbank market;
4) a transaction carried out in the name or on behalf of the units of the public finance sector referred to in article 9 of the Act of 27 August 2009 on Public Finance;
5) a transaction carried out by a bank associating cooperative banks, if information on the transaction has been provided by an associated cooperative bank; and
6) a transfer of ownership to secure assets, effected for the term of an ownership transfer agreement with the obliged institution.

The requirements indicated above are subject to the measures of article 2 sec. 1 Polish Act on Anti-Money Laundering, for example:

domestic banks; cooperative savings and credit unions; domestic payment institutions; custodian banks; investment companies; companies operating on a regulated market; foreign legal entities conducting brokerage activities on the territory of the Republic of Poland; investment funds; and insurance companies.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

The obliged institutions are required to apply financial security measures for establishing business relationships and occasional transactions. Financial security measures include: identifying the customer and verifying the customer's identity; identifying the beneficial owner; assessing (and, in some circumstances, obtaining information on the purpose and intended nature of the business relationship); and conducting ongoing monitoring of the business relationships of the customer.

The risk assessment is based on the type of customer, the geographic area, the purpose of the account, the type of products, services, and manners of their distribution, the level of assets to be deposited by the customer or the value of the transactions undertaken and the purpose, regularity or duration of the business relationship.

Firstly, obliged institutions are obliged to apply increased financial security measures when the client is referred to as having a higher risk of money laundering and terrorist financing. An example of situations that indicate a higher risk is: the customer is a legal person or an organisational unit without legal personality whose activity has the purpose of holding personal assets; and/or the business relationship is established in unusual circumstances.

Additionally, if the client is classified as a low risk entity, the obliged institution may then apply simplified financial security measures.

Institutions obliged during a business relationship with a politically exposed person apply additional measures such as obtaining senior management approval for establishing or continuing a business relationship with a politically exposed person, taking adequate measures to establish the source of wealth and the source of assets available to a given customer under the business relationship or a transaction and increased conduct of ongoing monitoring of the business relationships of the customer.

Other due diligence requirements are identifying the beneficial owner and taking reasonable measures to verify that person's identity, and determine the ownership and control structure-in the case of a customer being a legal person or an organisational unit without legal personality, assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship and conducting ongoing monitoring of the business relationships of the customer.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

The Polish Anti-Money Laundering Act prohibits making or continuing correspondence with shell banks to financial institutions referred to in article 2 para. 1 points 1–5, 7–11, 24 and 25 of the Polish Anti-Money Laundering Act. There are, for example, banks and other financial institutions.

3.9 What is the criteria for reporting suspicious activity?

An example of such activity can be:

1) strange customer behaviour (the client shows signs of nervousness and/or fear);
2) the client is observed or accompanied by suspects;
3) issuing orders by third parties;
4) handing cash to the customer at the cash register window by third parties;
5) frequent transactions – several transactions of the same type in one day;
6) an extraordinary way of transporting money;
7) money is deposited in a rare currency; and
8) an irrational choice by the client of the branch of the obligated institution located far from their place of residence or seat.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, there is a National Court Register in Poland, where data about legal entities and their management and ownership is available for everyone. In addition, the Central Register of Beneficial Owners will operate from October 13th, 2019. This register will contain information such as identification data of the beneficial owners and a member of a body or a partner authorised to represent the companies and partnerships.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, such information can be found on transfer orders.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Yes, it is permitted. Currently, a change that introduces dematerialisation of bearer shares in non-public (off-exchange) companies is being planned, i.e. disclosure in special registers, who, in what number and in which companies has such shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the Polish Act on Anti-Money Laundering is not applied to entities other than those specified in question 3.1.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No such requirements exist.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Within the European Union, the 5th AML Directive was passed. One of the changes that entail the introduction of new regulations is the limitation of the possibility of using anonymous pre-paid cards and the obligation to implement specific precautions in cooperation with entities from countries outside the European Union.

The 5th AML Directive also introduces a register of beneficiaries, which Poland decided to introduce into the Polish legal system together with the 4th AML Directive. Another change due to the 5th AML Directive which has already been implemented in Poland is the extension of the catalogue of obliged institutions to entities operating in the field of virtual currency trading.

In its entirety, the 5th AML Directive is to be introduced to the Member States by January 10, 2020.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

No, there are not.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

In 2013, the Counsel of Europe (Moneyval) carried out an evaluation of the Polish system of anti-money laundering and financing of terrorism.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The Polish Act on Anti-Money Laundering is publicly available in English. The English language version is available at the Ministry of Finance website https://www.gov.pl/documents/3297389/3574417/ustawa_tekst_EN__15062018-f__16072018.pdf.

Acknowledgment

The authors would like to thank Magdalena Bętkowska for her invaluable contribution to the writing of this chapter. Ms. Bętkowska graduated from the Faculty of Law and Administration at Adam Mickiewicz University in Poznań. She has organised and actively attended a number of Polish and international academic conferences and was awarded multiple rector's scholarships for outstanding academic achievements.

Wojciech Kapica

SMM Legal Maciak Mataczyński
Adwokaci Sp.k.
ul. Mokotowska 33/35
00-560 Warsaw
Poland

Tel: *+48 22 10 10 430*
Email: *wojciech.kapica@smmlegal.pl*
URL: *www.smmlegal.pl/en*

Wojciech is a uniquely qualified expert in the field of compliance, financial sector regulations, and regulatory relations with unmatched expertise in Poland. In his everyday work he assists leading Polish banks, investment firms and clearing institutions providing them with top quality advice in an effective and straight-forward manner. A specialist in banking law, capital law, insurance law, supervisory policy and corporate governance specific to regulated businesses, he has participated in preparations to implement CRD IV/ CRR (Basil III), EMIR and BRRD in Poland.

He has coordinated a number of licensing procedures concerning banks, brokerage houses and clearing institutions before Polish and foreign financial supervision authorities and has extensive experience in establishing effective compliance systems in financial institutions.

He graduated from the Faculty of Law and Administration of Warsaw University and completed a post-graduate programme in management and finance at the Warsaw School of Economics.

Zuzanna Piotrowska

SMM Legal Maciak Mataczyński
Adwokaci Sp.k.
ul. Mokotowska 33/35
00-560 Warsaw
Poland

Tel: *+48 22 10 10 430*
Email: *zuzanna.piotrowska@smmlegal.pl*
URL: *www.smmlegal.pl/en*

Zuzanna graduated from the Faculty of Law and Administration at the University of Warsaw.

Her key area of specialty is financial market regulation. Her extensive experience spans from regulations on anti-money laundering and terrorism financing (AML IV) to payment services (PSD II) and financial instruments (MIFID II).

She started her professional career while still at university, working with a law firm specialising in civil and criminal law. She also worked with a firm advising start-ups and e-commerce businesses before moving to an insurance company in 2016, where she focused on analysing liability for damage. From 2017 she has worked with a law-firm in Warsaw, specialising in broadly construed financial law.

She co-authored a commentary to GDPR entitled "RODO. Przewodnik z wzorami" (*Wolters Kluwer*) and a companion to a new AML Act (*Wolters Kluwer*, planned publication: October 2018).

SMM LEGAL

SMM Legal is one of the largest law firms in Poland, holding 13th place in the 2018 Rzeczpospolita law firms ranking. Our legal team includes five professors and a large number of PhD graduates, as well as graduates of the best universities in the world, such as Harvard Law School and Oxford University.

Strong expertise and extensive experience of our team members, including skilled lawyers previously working with regulatory authorities, put our Firm in a unique position to offer top quality legal and regulatory advisory to financial institutions. We offer services in the area of regulatory and legal advisory to banks, brokerage houses, clearing institutions and other financial businesses based on our experience in a variety of fields. Our lawyers are the authors of a practical guide to the new Act on preventing money laundering and financing of terrorism, which is the first such guide on the market.

Portugal

Tiago Geraldo

Tiago da Costa Andrade

Morais Leitão, Galvão Teles,
Soares da Silva & Associados, SP, RL.

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Public Prosecutor prosecutes at national level and is assisted by police agencies.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Anyone who converts or transfers funds – or intervenes or aids within such operations – in order to conceal their unlawful origin may be held liable for money laundering. Predicates offences include, e.g., tax evasion, bribery and corruption, influence peddling, trafficking (arms, organs, drugs) and any crime punishable with a minimum sentence of six months' imprisonment or a maximum sentence of five years' imprisonment.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes. The Portuguese criminal law applies provided that any stage of the money laundering process relates in any way with the Portuguese territory (e.g. funds transferred to Portuguese banks).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The public prosecutor – and the police agencies – have full competency regarding money laundering criminal offences. However, the Bank of Portugal, the Portuguese Securities Exchange Commission, the Registry and Notary Office, the Real Estate and Construction Authority and the Tax Authority, among others, are also responsible for investigating regulatory infractions related with money laundering offences.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is both corporate and natural person criminal liability for money laundering criminal offences and related regulatory offences.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The imprisonment penalty may range up to a maximum of 12 years, although this is always limited to the maximum sentence applicable to the predicate offence, if lower. In case of legal entities, the imprisonment sentence is converted into a fine penalty. One day of prison corresponds to a 10-day fine, and each day of fine corresponds to an amount of between €100 and €10,000, which the court shall set depending on the economic and financial situation of the convicted entity and its expenses with employees.

1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is 15 years (without prejudice of potential causes of interruption or suspension, which may impact the calculation of the maximum time period).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes, currently the enforcement applies only at national level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

If the Public Prosecutor has solid suspicions that the defendant may lack funds to guarantee the payments and debts related to the crime under investigation, it can issue a petition to the court and the latter may order the confiscation of the defendants' assets, even without criminal conviction.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, including directors.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

In the case of money laundering, there is no other way if not by a criminal (judicial) proceeding to settle the case. The records of the proceedings become public, if not early, at the trial stage.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Under the recent Law 83/2017, from August 18th 2017, the authorities responsible for imposing anti-money laundering requirements on financial institutions, depending on the type of institution, are the Bank of Portugal, the Portuguese Securities Market Commission, the Portuguese Insurance and Pension Funds Supervisory Authority and even the General Inspectorate for Finance. On other businesses, the responsible authorities are professional associations and other government agencies and authorities with supervisory powers within the relevant business sector.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes, our legal framework allows self-regulatory organisations or professional associations to impose regulatory provisions or rules concerning anti-money laundering requirements in development of the above-mentioned Law 83/2017, which is based on the model of a risk-based approach.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, some professional associations are responsible for anti-money laundering compliance and enforcement against their members, including the legal requirements.

2.4 Are there requirements only at national level?

No, there are also requirements at the European Union level. The aforementioned Law 83/2017 intends in fact to transpose Directive (EU) 2015/849 (4th AML Directive).

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see question 2.1 above: the agencies/authorities responsible for compliance and enforcement of anti-money laundering requirements are the same. There are currently no criteria for examination which are publicly available.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, there is a Financial Intelligence Unit ("FIU") that integrates the bodies of the Portuguese Criminal Police. FIU is responsible for preparing and updating statistical data related to suspicious transactions that have been reported and their results, and data related to transnational information requests that have been sent, received or refused by the FIU. Further information may be found at http://portalbcft.pt/.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

In what concerns regulatory offences, under the Law 83/2017, the statute of limitations is five years, with possible suspension (and interruption) of this deadline in certain cases.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Failure to comply with the regulatory/administrative anti-money laundering requirements may lead to penalties of up to €5,000,000, depending on the nature of the entity, which may be aggravated up to double of the economic benefit obtained with the infraction or up to 10% of the annual volume of business in certain cases.

Penalty provisions include: (i) the illegitimate disclosure of information, communications, analyses or other elements, to clients or third parties; (ii) the disclosure or improper favouring of identity discovery of those who provided information, documents or elements concerning suspicious transactions; and (iii) the disobedience of orders or legitimate instructions from sectorial authorities when issued in the context of their duties, or, by any means, creating obstacles to their execution.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

It is possible to impose on both individuals and legal entities for regulatory offences, besides monetary fines, additional sanctions such as: (i) losing for the State the object of the offence and the economic benefit derived from it; (ii) closing of the establishment where the agent develops the activity or job related to the offence, for a period up to two years; (iii) prohibition of professional activity or job related to the offence, for a period up to three years; (iv) prohibition of exercising certain directorial and representative functions, among others, in obliged entities to the supervision or control by a sectorial authority, for a period up to three years; and (v) publication of the final or definitive conviction.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

There are both administrative and criminal penalties in case of violations of anti-money laundering obligations. Besides the crime of money laundering itself, the crimes related to violations of anti-

money laundering obligations include (i) illegitimate disclosure of information, (ii) disclosure and improper favouring of identity discovery, and (iii) disobedience of lawful orders or instructions from the competent agencies/authorities.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process for assessment and collection of sanctions is carried out by several different government agencies and authorities, listed above (see question 2.1 above), depending on the type of institution or obliged entity. The process has an entire administrative procedural stage where the individuals or legal entities may defend themselves after a formal indictment is issued. If the competent authority decides to impose a sanction on an individual or legal entity, the latter may appeal to a judicial court.

Not all administrative resolutions become public, although the secrecy regime, applicable as a general rule to the proceedings in their administrative stage, elapses with the final decision.

Several financial institutions have challenged penalty assessments in judicial and regulatory proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The financial institutions subject to anti-money laundering requirements are: (i) all kind of banks, including credit, payment and electronic money institutions; (ii) investment firms and other financial companies; (iii) self-managed securities and real estate investment companies; self-managed venture capital companies, investors in venture capital, social entrepreneurship companies, venture capital investment management companies, venture capital investment companies and specialised alternative investment companies; (iv) securitisation companies; (v) companies which commercialise contracts relating to the investment in tangible assets to the public; (vi) consultants for investment in securities; (vii) pension fund management companies; and (viii) companies and insurance intermediaries with activity in life insurance. The requirements apply also to any branches located in Portuguese territory pertaining to any previous entities headquartered abroad, as well as to any offshore financial centres, to payment institutions headquartered in another EU Member State, when operating in Portuguese territory through agents, or any electronic money institutions headquartered in another EU Member State, when operating in Portuguese territory though agents or distributors. Any of the previously mentioned entities operating in Portugal under the free provision of services may have to render information to the relevant sector authority. The agents and distributors, whether natural or legal persons, are also subject to anti-money laundering requirements.

The following professional activities are also subject to anti-money laundering requirements: (i) providers of gambling, lottery or betting services, whether in an establishment or online; (ii) non-financial real estate entities; (iii) auditors, external accountants and tax advisors, whether as natural or legal persons; (iv) lawyers, solicitors, notaries and any other independent legal professionals performing certain activities; (v) trust or company service providers in certain activities; (vi) other professionals who intervene in operations of selling and buying rights over professional sport's players; (vii) economic operators exercising auction or lending activities; (viii) economic operators importing or exporting rough diamonds; (ix) entities authorised to exercise the activity of transportation, custody, handling and distribution of funds and values; and (x) other entities/persons trading in goods where payment is made in cash.

Finally, some requirements are also applicable to crowdfunding platforms, of the loan and capital type, and managing entities of crowdfunding platforms, in the categories of donation and reward and non-profit organisations.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Crypto exchanges are not entities subject to anti-money laundering requirements for the purpose of Law 83/2017. However, the EU Directive 2018/843, from May 30th 2018, now stipulates that virtual currency exchanges and custodian wallet services shall be considered as obliged entities, forcing Portugal to amend said Law before January 10th 2020, extending the obligations provided therein to those service providers. Furthermore, the Bank of Portugal issued the circular letter 11/2015/DPG, endorsing credit, payment and electronic money institutions to refrain from buying, owning or selling virtual currency, to prevent a variety of risks, including money laundering. The Bank of Portugal also restated that financial institutions must assess the transfers of funds with the origin and destination on virtual currency trading platforms, in the light of the current rules of prevention of money laundering and terrorism financing. These rules include several obligations, such as identifying customers, recordkeeping of clients and operations, examining and communicating suspicious operations and adopting an internal compliance system.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Financial institutions must maintain an independent, permanent and effective "function of compliance" to monitor and enforce internal control procedures regarding anti-money laundering and other risks. The Bank of Portugal defines several requirements for this "function", beginning with full independence and adequacy.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There are no thresholds for reporting transactions suspected of money laundering. All suspicious transactions ought to be reported, regardless of the amounts involved.

The reporting of suspicious transactions is directed at the General Prosecution Office and the Financial Information Unit and must be performed as soon as the suspicion arises and whether the operation has been merely proposed or attempted, if it is under course or it has

already been concluded. The report must, at least, include: (i) the identification of the natural or legal persons involved, as well as any known information on their activity; (ii) the specific procedures of enquiry and analysis carried out; (iii) the characterising and descriptive elements of the relevant or envisaged operation; (iv) the specific suspicious factors identified by the entity; and (v) a copy of all supporting documentation obtained through due diligence.

All entities subject to anti-money laundering requirements must keep records for a period of seven years, from the moment the client was identified, or, in case of a business relationship, from the moment it terminated, of all documents and data obtained from clients, as well as all documents pertaining to the client's files and accounts, and all documentation produced in compliance with legal requirements, such as the documents gathered and sent to the relevant authorities to comply with the reporting duty.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

According to ministerial order 310/2018, from December 4th 2018, all entities subject to anti-money laundering requirements must communicate to the Central Department of Criminal Investigation and Prosecution and to the Financial Intelligence Unit cash transactions of €50 or more, but also transactions of those values by cheques or any other paper document drawn on the payment service provider. In addition, fund transfers of €50,000 or more to or from risky jurisdictions – identified in specific lists which bind the Portuguese State – early repayment of funds and insurance policies of €50,000 or more and operations or transactions of gambling services providers must be communicated as well. An exemplificative list of red flags can be found at http://portalbcft.pt/.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

The anti-money laundering requirements are applicable to all transactions, regardless of being national or cross-border operations. Within the EU there is a level playing field regarding applicable requirements and authority control and information sharing. If the transaction is carried out in the context of a correspondent relationship or with a high-risk third party, even though there are no specific requirements for reporting, there is an increased risk profile to the operation, leading to enhanced due diligence measures.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Entities subject to anti-money laundering requirements must comply with customer identification and due diligence requirements whenever they establish a business relationship or when carrying out an occasional transaction that (i) amounts to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked, or (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council, exceeding €1,000.

For providers of gambling, lottery or betting services, the threshold corresponds to transactions amounting to €2,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

Finally, such requirements apply whenever there is a suspicion of money laundering practices, regardless of any derogation, exemption or threshold or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Customer identification and due diligence require obtaining elements of identification, the activity exercised, documents to verify such elements and information regarding the purpose and nature of the intended business relationship. When the specific risk profile of the client or the characteristics of the operation may justify it, information should be obtained regarding the origin and destination of the funds. There must be a constant monitoring of the business relationships to ensure that the operations carried out in its course are consistent with the knowledge the entity has of the activities and risk profile of the client and the origin and destination of the movement of funds.

Due diligence requirements are enhanced whenever there is a transaction involving high-risk third countries, non-face-to-face business relationships or transactions, politically exposed persons or other high public and political offices, life insurance policies or cross-border correspondent relationships with third country institutions, as provided in annexes I and II to the Regulation 2/2018, from September 11th 2018, of the Bank of Portugal.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Law 83/2017 prohibits financial entities from establishing or maintaining correspondent relationships with shell banks or to establish or maintain correspondent relationships with other financial institutions which allow their accounts to be used by shell banks.

3.9 What is the criteria for reporting suspicious activity?

If an entity knows, suspects or has enough grounds to believe that certain funds or other assets, regardless of the amount involved, were originated by criminal activity or are related to terrorism financing, such entity must report the suspicious activity.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

There is a public corporate registry that can be accessed through a code for each individual company. The legislation regarding a central register for beneficial owners entered into force on November 19th 2017. The purpose of this register is to provide, through different levels of access, information about the beneficial ownership of legal entities, amongst others, to financial institutions and other entities which are subject to anti-money laundering requirements, and to customer due diligence responsibilities.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Accurate information on originators and beneficiaries will depend on the client's risk profile and the features of the operation.

In the specific case of funds transfer not associated with an account, the financial institution of the originator or the beneficiary must collect a certain amount of information, depending on the type of the entity, regarding the originator or beneficiary's identification, if the transfer amounts to €15,000 or more (according to Regulation 5/2013 from the Bank of Portugal).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No, not since 2017.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes, there are certain requirements that are specific to providers of gambling, lottery or betting services, regarding, for example, the form of prize payment. Specific requirements also apply to legal professionals, although there is a derogation of the reporting duty whenever the services provided for the client are in the context of a judicial process.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Under Portuguese jurisdiction, trusts can only be registered in the free trade zone of Madeira, being applicable anti-money laundering requirements such as the gathering of information on their beneficial ownership, to be declared to the Central Register of Beneficial Owners.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Besides from Regulation 2/2018, from September 11th 2018, of the Bank of Portugal, there are other sectorial authorities which already proposed and published additional measures, such as the Economic and Food Safety Authority. Other sectorial authorities are preparing additional regulatory instruments, such as the Portuguese Securities Exchange Commission.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

In the last FATF evaluation (December 2017), Portugal was considered to have a sound legal framework in place to combat money laundering. According to that evaluation, Portugal was deemed Compliant for 12 and Largely Compliant for 22 of the FATF 40 Recommendations. The areas of non-profit organisations, correspondent banking, wire transfer, customer due diligence of designated non-financial businesses and professions, transparency and beneficial ownership of legal persons were deemed partially compliant.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

FATF conducted an onsite visit (March 28th–April 13th 2017) and produced a Mutual Evaluation Report in December 2017, mentioned above.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The AML/CFT Coordination Commission, established in 2015, is responsible for the overall policy coordination and implementation of AML, CFT and counter-proliferation financing measures. Relevant legislation and guidance can be accessed in their homepage, at the following link: http://portalbcft.pt/ (not available in English). Some sectorial authorities have internet pages in English, such as the Bank of Portugal (https://www.bportugal.pt/), but usually the legislation is not translated into English.

Tiago Geraldo

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Rua Castilho, 165
1070-050 Lisboa
Portugal

Tel: +351 213 817 400
Email: tgeraldo@mlgts.pt
URL: www.mlgts.pt/en

Tiago Geraldo joined the firm in 2008. He is a member of the litigation department.

His practice focuses in criminal litigation, including regulatory offences, especially in the economic and financial fields.

He also provides collaboration within the areas of competition law, corporate law, labour law and tax law, regarding criminal or quasi-criminal aspects.

In parallel, he has been counselling companies and individual clients on a variety of matters related to compliance and regulatory enforcement, in different sectors such as banking, capital markets, energy, telecommunications and media.

He is an Assistant Teacher of the Law Faculty of the University of Lisbon, teaching Criminal Law.

He is also a Researcher at the Center for Research in Criminal Law and Criminal Studies (IDPCC) and founding associate of the Institute of Criminal Law and Criminal Studies (IDPCC) of the Law Faculty of the University of Lisbon, participating as guest lecturer in conferences and postgraduate courses on matters related to criminal law, criminal procedure, regulatory offences and compliance.

Tiago da Costa Andrade

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Rua Castilho, 165
1070-050 Lisboa
Portugal

Tel: +351 213 817 400
Email: tcandrade@mlgts.pt
URL: www.mlgts.pt/en

Tiago da Costa Andrade joined the Firm in September 2018. He is a member of the litigation and arbitration team.

Was Teaching Assistant, having collaborated in Criminal Procedural Law, in the Law Faculty of the University of Coimbra (2017).

Is the author of a published article and intervenes in international conferences as guest speaker in the fields of Criminal Law and Criminal Procedural Law.

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

Morais Leitão is a leading full-service law firm in Portugal, with a solid background of decades of experience. Broadly recognised, Morais Leitão is a reference in several branches and sectors of the law on national and international level.

The firm's reputation amongst both peers and clients stems from the excellence of the legal services provided. The firm's work is characterised by a unique technical expertise, combined with a distinctive approach and cutting-edge solutions that often challenge some of the most conventional practices.

With a team comprising over 250 lawyers at a client's disposal, Morais Leitão is headquartered in Lisbon with additional offices in Porto and Funchal. Due to its network of associations and alliances with local firms and the creation of the Morais Leitão Legal Circle in 2010, the firm can also offer support through offices in Angola (ALC Advogados), Hong Kong and Macau (MdME Lawyers) and Mozambique (HRA Advogados).

Romania

Simona Pirtea

Mădălin Enache

Enache Pirtea & Associates S.p.a.r.l.

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In Romania, all the prosecution is conducted by the Public Ministry, organised in Prosecutors' Offices with the courts of law (Ordinary Courts, Tribunals, Courts of Appeal, the High Court of Cassation and Justice "HCCJ").

The Prosecutors' Offices with Tribunals have general competence to prosecute money laundering crimes. However, any other superior Prosecutors' Office can also prosecute money laundering if, in the investigation of other crimes within their competence, they uncover such deeds committed by the same person or having a strong link to these. In addition, the specialised Prosecutors' Offices (National Anticorruption Directorate – "NAD" and the Directorate for Investigating Organized Crime and Terrorism – "DIOCT") can prosecute money laundering if the predicate offence is within their competence.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Money laundering is provided by the Law no. 656/2002 ("Law 656"), art. 29 defining it as one of the following conducts:

- conversion or transfer of property, knowing that such property is derived from criminal activities, for the purpose of concealing or disguising the illicit origin of that property or of assisting any person who was involved in the criminal activity to avoid the legal consequences of his action;
- the concealment or disguise of the true nature of the origin, location, disposition, movement, ownership or rights with respect to such property, knowing that such property is derived from criminal activities; and
- the acquisition, possession or use of property, knowing that the property is derived from criminal activities.

Law 656 does not limit the range of crimes which can be considered predicates for money laundering. As a result, any offence that leads to obtaining "dirty" money or properties can be the predicate for money laundering.

Tax evasion is a recurrent predicate crime for money laundering, as there is a very wide range of criminal cases having as object charges/accusations of tax evasion together with money laundering. Receipt of bribes or misuse of EU funds are other common predicate crimes.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

As per art. 9 from the Criminal Code, Romanian criminal law (Law 656 included) applies to crimes committed outside Romanian territory by a Romanian citizen/legal entity if the act is also outlawed by the criminal law of the country where it was committed or if it was committed in a location that is not subject to any jurisdiction.

As stated in the Preliminary Ruling Decision nr. 16/2016 of the HCCJ, Romanian Criminal law does not require a prior or simultaneous conviction for a predicate offence in order to obtain a conviction for money laundering, thus money laundering is an autonomous crime. *A fortiori*, money laundering of the proceeds of foreign crimes is punishable (especially if there is a conviction decided where the offence was committed).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Besides the Prosecutors' Offices (as presented above), investigations can be conducted at a preliminary stage by the National Office for Prevention and Control of Money Laundering ("NOPCML"), which is the Romanian FIU and leading supervisory authority regarding money laundering. As soon as it identifies indications/suspicions of money laundering (as a crime), NOPCML must immediately inform the Prosecutors' Office to launch an official investigation. NOPCML has also the competence to collect and process relevant information as to facilitate the activity of the prosecutors, as per their request.

1.5 Is there corporate criminal liability or only liability for natural persons?

Starting from 2006, the Romanian Criminal law introduced the criminal liability for legal entities if the crimes are committed in the performance of the object of activity of legal entities or in their interest or behalf.

This is a general provision, hence it also applies to money laundering crimes. The corporate criminal liability does not exclude the criminal liability of the involved natural persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

For individuals, money laundering is punishable with three to 10 years of imprisonment. For legal entities, the main penalty is the fine, which can be set at any value from RON 18,000 (app. EUR 3,900) to RON 1,500,000 (app. 326,000 EUR).

1.7 What is the statute of limitations for money laundering crimes?

For money laundering, the general statute of limitations is eight years. However, the special statute of limitations of 16 years might also apply (there are hard debates at present on such applicability).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Romania is a national state, the reason for which there is only one authority – the Prosecutors' Office with the HCCJ – who can conduct criminal investigations. As mentioned, this is organised with central and local structures, including specialised directions (NAD and DIOCT, also with local structures).

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Asset forfeiture can be ordered by any prosecutor and court of law against the goods of a defendant, while confiscation can only be ordered by a court of law, along with a criminal conviction.

The object of the forfeiture/confiscation can be any money, goods or assets which were produced by the criminal activity and were: used in any way or intended to be used in the activity; used to ensure the perpetrator's escape; given to reward the perpetrator; acquired by perpetrating the offence; or if their possession is prohibited by the law. If the goods were transferred to third parties of good faith, cannot be found or they have been alienated, the authorities can confiscate the equivalent of their value or the price. Without a criminal conviction, confiscation can be instituted on the property of third parties only if it is a direct or indirect product of the crime.

Furthermore, in 2015 it was established, under the authority of the Ministry of Justice, the National Agency for the Management of Seized Assets ("NAMSA"), in order to facilitate asset recovery by combining the support of the criminal prosecution bodies with the attributes of international cooperation, management of seized assets and social reuse of confiscated assets.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

There have been several criminal investigations of bank executives and officers for collusion to money laundering yet there exists no public record of any conviction.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

If the individual or the legal entity is considered guilty, the criminal actions can be resolved only in front of a Court of law. No settlement can be concluded only by the prosecutor/other authority and the perpetrator.

However, Romania has introduced in 2014 the possibility for defendants and prosecutors to conclude a Deferred Prosecution Agreement, by which the defendant admits guilt and recognises the accusations in exchange for a diminished penalty (usually a prison conviction with suspended execution), but a Court must still verify the lawfulness and the terms of the DPA and admit it.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Only Parliament can impose legislation (as is Law 656 for AML). Financial institutions are also regulated by specific bodies, which can complete or detail, through general applicability Orders, these norms. The authorities invested with the supervision of the compliance with the legal requirements are:

a) the prudential supervision authorities (as Romanian National Bank or Financial Supervisory Authority), for the entities that are subject to their supervision, including the branches of foreign legal persons that are subject to a similar supervision in their country of origin;

b) National Anti-Fraud Agency, with tax and financial control attributions; and

c) NOPCML, as provided by Law 656.

The legal requirements consist of the following main obligations: KYC rules; designation of AML officer; reporting of suspicious transactions to NOPCML; freezing of operations pending NOPCML clearance; safeguarding all relevant evidence of suspicious transactions; and not informing the clients about any AML investigations.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

No, the AML requirements are imposed only by the law. Nevertheless, self-regulatory organisations or professional associations can elaborate guides and recommendations for compliance with AML requirements. For example, *The Guide for the best practices of reporting suspect transactions which might involve money laundering or terrorism financing* released by the Chamber of Financial Auditors of Romania in 2016.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The leading structures of the independent legal professions (*e.g.*

auditors, tax or accounting consultants, lawyers, public notaries) must designate one or several AML officers as per Law 656. These persons must establish adequate policies and procedures (KYC, AML reporting, secondary and operative recordkeeping, internal control, training, etc.) in order to prevent and stop any money laundering and terrorism financing operations by its members. Indifferent of the cooperation existing on AML between these structures and NOPCML, they are not directly responsible for non-compliance of their members.

2.4 Are there requirements only at national level?

Yes, with general applicability.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see question 2.1 for the authorities mentioned, based on the provisions of Law 656 and derivative legislation.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

NOPCML is Romania's FIU, with duties of preventing, sanctioning or reporting money laundering activities. NOPCML receives/requests, analyses and processes information originating from institutions/entities having AML obligations.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

From the moment when the violation act has ended, the authorities have six months to apply a sanction/contravention, which must be communicated to the offender by a further maximum of two months. If the deed is considered a crime, the general (and possibly special) statute of limitations applies (please see question 1.7 above).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Breaching the provisions of Law 656 may constitute a contravention, sanctioned with up to RON 50,000 (app. EUR 11,000) fine.

The following misconducts may be sanctioned with the highest fine: failure to transmit requested information to NOPCML within 15 days (or 48 hours, in urgent matters); failure to comply with the adequate KYC measures or with the obligation to designate an AML officer; (for credit and financial institutions) opening/operating an anonymous account or an account which does not permit a proper identification of the client; and (for the institutions and the authorities with supervision duties) failure to accomplish their duties.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The individuals cannot be the subject of other types of sanctions in an administrative (and not criminal) procedure.

For legal entities, Law 656 establishes the following accessory sanctions for non-criminal violations: confiscation of the goods that have been used in, destined to be used in or obtained from committing the violation; suspension/annulment of the authorisation to engage in the activity; withdrawal of the licence for certain operations or for foreign trade activities; freezing of bank account; suspension of the activity of the entity; shutting down the entity's unit. Moreover, for the entities targeted by the prudential control, the supervision authorities (RNB or FSA) can impose specific sanctions for their type of activity.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

The penalties can be administrative, civil, or disciplinary. In addition to this, criminal sanctions can be applied for violating the interdiction to transmit information regarding the money laundering or terrorism financing and in case of any leaks of information to the client about an ongoing NOPCML investigation, both to the financial institutions and/or their representatives. Moreover, as an auxiliary penalty, the individuals can be banned from the exercise of the profession or occupation they have used for committing the crime.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

a) No, the general practice is that the resolutions of penalty actions are not public.

b) Yes, it is a common practice to challenge any penalty that is imposed by the authorities.

The administrative sanctions can be applied by NOPCML or by the prudential supervision authorities (for the entities supervised by them) and they can be appealed in Court, like any other administrative sanction in the Romanian legal system.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

According to art. 10 of Law 656, the following entities are scrutinised:

a) credit institutions and branches in Romania of the foreign credit institutions;

b) financial institutions, as well as branches in Romania of the foreign financial institutions;

c) private pension funds administrators, in their own behalf and for the private pension funds they manage, marketing agents authorised for the system of private pensions;

d) casinos;

e) auditors, natural and legal persons providing tax and accounting consultancy;

f) public notaries, lawyers and other persons exercising independent legal professions, when they assist in planning or executing transactions for their customers concerning the purchase or sale of immovable assets, shares or interests or trade funds, managing of financial instruments or other assets of customers, opening or management of bank, savings, accounts or of financial instruments, organisation of contributions necessary for the creation, operation, or management of a company, creation, operation, or management of companies, undertakings for collective investments in transferable securities, other trust activities or when they act on behalf of and their clients in any financial or real estate transactions;

g) service providers for companies or other entities, other than those mentioned in para e. or f.;

h) persons with duties in the privatisation process;

i) real estate agents;

j) associations and foundations; and

k) other natural or legal persons that trade goods and/or services, provided that the operations are based on cash transactions, in RON or foreign currency, whose minimum value represents the equivalent in RON of EUR 15,000, indifferent if the transaction is performed through one or several linked operations.

The credit institutions and the financial institutions must have internal rules and procedures for KYC and swift collaboration with NOPCML, on demand.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

At this moment, no cryptocurrency AML-related requirements were initiated in Romania. However, individuals have an obligation to declare the incomes from the transactions that involve cryptocurrencies and to pay a tax consisting of 10% of the income (if the income from one transaction is higher than RON 200 or if the total annual income is higher than RON 600).

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All entities subject to Law 656 must adopt adequate AML measures and apply risk-based standard/simplified/additional customer due diligence measures, in which to identify, where applicable, the real beneficiary. The financial institutions must also apply AML measures of customer identification to foreign branches and subsidiaries.

In addition, reporting entities must also appoint one or multiple officers to handle the relation with NOPCML; these persons must have specific responsibilities and NOPCML should be informed about their names and the nature and limits of their specific duties.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Reporting entities must implement secondary or operative recordkeeping policies, designed for internal control, risk assessment and management, as to obstruct and prevent operations suspected of money laundering. When client identification is required, these entities have the obligation to keep copies of identity documents for a period of five years, from the date when the relationship with the client is terminated.

Reports to NOPCML must be filed within 10 working days from the internal or external transaction(s) with cash, in RON or foreign currency, whose minimum threshold represents the equivalent in RON of EUR 15,000, irrespective of whether the transaction is performed in only one operation or in several operations that seem interconnected.

The new law proposal reduces the term from 10 to three working days.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, there are none.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There are no specific obligations – the general rules of reporting apply.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Law 656 stipulates three possibilities to customer-related obligations (especially KYC rules), chosen on a risk-based approach: standard; simplified; or supplementary.

The standard provisions apply whenever a business relationship is initiated/a new client is involved: for an occasional transaction of minimum EUR 15,000; when there is reasonable doubt that the transaction is destined to launder money/fund terrorism; or regarding the information provided by the client.

The simplified provisions apply when they refer to insurance claims, pension funds, electronic signature transactions, when the client is an EU financial institution, or in any other situation where there is a low risk of money laundering or terrorism financing.

The supplementary provisions apply when there is an increased risk of money laundering because: the other party is not physically present during the transaction; it is established a correspondent relationship with non-EU/non-EEA credit institutions; or the other party is a politically exposed person.

The standard measures are:

a) Identifying the client and verifying his identity in trustworthy sources, including documents.

b) Identifying the real beneficiary and risk-based verification of his identity, as to guarantee sufficient knowledge over the entity's ownership and control structure.

c) Obtaining information about the purpose and the nature of the business.

d) Continuously monitoring the business relationship, including analysing transactions, to ensure that they correlate with the information about the client, his risk-based/activity profile and the source of funds. The documents, data and information should always be updated.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Credit institutions are prohibited to enter into a banking relationship with a shell bank or with a credit institution that is known to allow its accounts to be used by a shell bank. In case there is an ongoing relationship, the credit institution must stop it immediately. All credit institutions are subject to this prohibition.

3.9 What is the criteria for reporting suspicious activity?

Law 656 only defines suspicious transactions as operations apparently not having economical/legal character or having (or being suspected of having) an unusual nature in relation to the activities of a client of one of the reporting entities. All suspicious transactions must be reported to ONPCSB.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The Romanian Government, mainly through the National Trade Registry Office, keeps detailed information regarding a company which any interested person can request access to (*e.g.* ownership structure, management, funding, financial records, etc.)

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

When sending money from an associated account, the payment order must include the full names and bank accounts of the originators and the beneficiary. Additional information (the fiscal or personal identification number) must be included if the beneficiary of the payment order is the National Treasury.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Under the provisions of the Law no. 31/1990, a joint-stock company has the liberty to decide whether the shares are nominative or bearer. Although bearer shares are legal, their existence in a company's structure can signal a "red flag" for the potential business partners and they might not be willing to engage in a business relationship for this reason. In addition to this, numerous auctions in the public sector allow only the participation of companies with nominative shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the general rules of reporting apply.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

There are none that are applicable.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

In November 2018, a new AML Law has been adopted, which implements the EU Directive 2015/849/UE. The most important changes which have not been presented above are:

- the obligation to declare the real beneficiary of the associations and foundations and the creation of a Registry with the real beneficiaries from the country;
- the definition of new terms, the most important one being "self-regulatory organisation";
- the bailiffs are introduced in the category of independent legal professions that are subjects of the AML law;
- the standard provision of the KYC rules will also be mandatory to all transfers of funds (as defined in the art. 3 pt. 9 of the EU Regulation 2015/847) exceeding EUR 2,000;
- the maximum administrative penalty will increase to 150 RON or even more if the misconduct is committed by a credit or financial institution in a serious, repeated or systematic way (up to 200 RON for individuals and 5,200 RON + 10% of the total income from the closed financial period for legal entities); and
- the prohibition of bearer shares in joint stock companies.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Certain recommendations regarding mainly bearer shares and publicity of sanctions have not been implemented yet, but the prohibition of the bearer shares is applicable.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The last Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards in Romania was undertaken by FATF (through MONEYVAL) in 2008. However, the last review of Romanian AML legislation was conducted by MONEYVAL in 2017.

Furthermore, in 2016 Romania was deemed a Jurisdiction of Concern by the US Department of State 2016 International Narcotics Control Strategy Report (INCSR).

In addition, Romania is still under scrutiny of the EU through the MCV (Mechanism for Cooperation and Verification) for the Justice System, certain recommendations being made as to strengthen the fight against corruption, including better capabilities of recovering the proceeds of crime and avoiding benefits from money laundering in relation to white-collar criminality.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The NOPCML website contains the main useful documents in this respect: http://www.onpcsb.ro/english-documents-onpcsb/relevant-legislation.

Simona Pirtea

Enache Pirtea & Associates S.p.a.r.l.
32 Pictor Ion Negulici Street
1st District, Bucharest
Romania

Tel: +40 740 137 358
Email: simona@enachepirtea.ro
URL: www.enachepirtea.ro

Professionalism accompanied by strategic thinking and absolute dedication are the attributes which describe Simona's activity as a lawyer. She is a well-respected Criminal Law practitioner, with more than a decade of intensive professional activity in the legal and the intelligence fields, having proven her strong technical knowledge and consistent business-oriented approach throughout a wide array of complex cases.

Simona is recognised for her straight-forward and innovative legal approach, as well as for her business-integrated advice. Based on her extensive experience in criminal law and risk management, and by using her knowledge and know-how obtained in this field, she has forwarded her practice conducting several major projects in compliance and regulatory.

Due to her very professional expert opinion and legal advice in complex or sensitive corporate matters, Simona has become a reputed counsellor for companies confronted with internal disorders or mismanagement situations. She has extensive expertise in dealing with important multinational companies, being also highly experienced in working with governmental and European institutions on matters regarding national security, economic strategies, strategic planning and risk management.

Simona is also notable for being a lecturer with the Superior Institute of Law and Economics Barcelona, Spain, and for having won numerous awards for her business-oriented approach as a business criminal lawyer.

Mădălin Enache

Enache Pirtea & Associates S.p.a.r.l.
32 Pictor Ion Negulici Street
1st District, Bucharest
Romania

Tel: +40 723 323 541
Email: madalin@enachepirtea.ro
URL: www.enachepirtea.ro

Mădălin has practised extensively and quasi-exclusively in high-level white-collar and business criminal cases since 2006, acquiring first-class professional expertise in some of the most difficult and media-scrutinised criminal investigations and trials, being known in the field as one of the highest skilled practitioners, building a solid reputation as a leading criminal law attorney and is acknowledged and recognised by clients and global legal publications (*Chambers Europe*, *The Legal 500*, etc.).

Mădălin counselled, assisted and represented renowned international and Romanian corporate clients, key figure businessmen and executives, and high-profile politicians involved in a wide range of cases in front of the criminal investigation authorities or courts of law, at the highest level of jurisdictions, with a focus on mainly corruption cases, financial and fiscal frauds, embezzlements of public/EU funds, money laundering, abuse of office, etc.

Due to his practical and business-focused approach, Mădălin is a valued lecturer on criminal law topics, having also published several specialised articles, in national and international publications, on different relevant topics in the criminal domain, especially in the areas of antibribery, money laundering and business crimes.

ENACHE PIRTEA & ASOCIAȚII
BUSINESS AT LAW

Enache Pirtea & Associates S.p.a.r.l. was set up in 2017 in Bucharest, after the merger of the specialised criminal law boutique offices of two of the most prominent "new wave" criminal law practitioners, Mrs. Simona Pirtea and Mr. Mădălin Enache, both with across-the-board experience in "white-collar" criminality matters.

The Firm's focal area of activity is Criminal Law – White Collar & Business Crime, in all its three main components: defence during criminal investigation and prosecution; criminal litigation; criminal consultancy and counselling (compliance & regulatory).

Over the past 14 years we have developed unparalleled practical skills, forged in the midst of some of the fiercest and most scrutinised top-level court battles and prosecutorial inquiries, either working for foreign or local corporate clients and for their executives and officers, or acting on behalf of business men, public figures, politicians or officials.

Be it corruption crimes or money laundering, economic criminality or abuse of office, embezzlement of EU funds or cybercrimes, copyright or environmental criminal breaches, we have across-the-board experience and knowledge. Proven by our results.

Russia

Rustam Kurmaev

Dmitry Gorbunov

Rustam Kurmaev and Partners

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Criminal cases involving money laundering are investigated by investigators from the agencies of the Ministry of the Interior Affairs, or sometimes by officers of the Investigative Committee of the Russian Federation or the Russian Federal Security Service. Additional assistance is provided by the Public Prosecution Office of the Russian Federation and the Federal Service for Financial Monitoring (*Rosfinmonitoring*).

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

In order to establish that a criminal offence has taken place, it must be shown that (1) a transaction involving cash or financial instruments has been entered into, (2) there has been an intention to create an impression of legitimate possession, (3) cash has been acquired through illegal means, and (4) the alleged offender is aware that the origin of the cash in question is illegal. A predicate offence is any offence as a result of which a person acquires cash or property illegally. In line with the latest FATF recommendations of February 2012, the list of predicate offences was supplemented to include tax crimes.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Acts involving money laundering committed outside the Russian Federation but aimed against the interests of the Russian Federation or its citizens are punishable in accordance with the Russian criminal law if a person who has committed these acts has not been convicted by a foreign court. Where cash transactions involve proceeds acquired as a result of crimes committed abroad, the offender is to be prosecuted in the usual manner.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Criminal cases involving money laundering are investigated by investigators from the agencies of the Ministry of Home Affairs, the Investigative Committee of the Russian Federation or the Russian Federal Security Service. Prosecution in court is conducted by a state prosecutor who is an officer of the Public Prosecution Service of Russia.

1.5 Is there corporate criminal liability or only liability for natural persons?

Only natural persons can be prosecuted in the Russian Federation.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalty for committing a money laundering offence is imprisonment for up to seven years with (or without) a fine of up to one million roubles or up to five years' worth of wages of the offender.

1.7 What is the statute of limitations for money laundering crimes?

In most cases the statute of limitations for such crimes is 10 years from the date an offence was committed.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Criminal prosecution is within the exclusive jurisdiction of federal agencies; no prosecution of any crimes is conducted at regional level.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

Confiscation of property is not amongst the sanctions imposed for money laundering by the Russian Criminal Code. The criminal proceeds may, however, be confiscated and returned to the victim as part of the investigation into how the funds have been acquired. As part of the civil proceedings, a victim of the crime may claim damages from the perpetrator. Court rulings are enforced by the Federal Bailiffs Service. In certain cases, the Public Prosecution

Office of the Russian Federation may initiate action to detinue (seize) property obtained by the government employees with funds that are not supported by any proof of income.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, such examples exist. For instance, Leninsky District Court in Chelyabinsk found the former director of the "Na Gagarina" branch of VTB-24 in Leninsky District of Chelyabinsk A. Kiselev and a local entrepreneur O. Baskildin (*pro rata* for their respective roles) guilty of 24 counts of offences under Article 159(4) (grand-scale fraud committed by a group of persons using their official position) and Article 174.1(2) of the Russian Criminal Code (laundering of a large amount of funds acquired by a person as a result of committing a crime).

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal procedural legislation envisages the possibility of dropping criminal charges on non-exonerating grounds at pre-trial proceedings (e.g. due to a pardon). Such facts are not secret but are not subject to mandatory publication.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The Federal Financial Monitoring Service is the Russian agency issuing, and monitoring compliance with, legislative acts in the area of anti-money laundering. In addition, the activities of financial institutions are monitored by the Central Bank of Russia.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Current Russian legislation does not provide for the possibility for SROs to impose anti-money laundering requirements.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Current Russian legislation does not provide for the possibility for SROs to monitor compliance of their members with anti-money laundering requirements, therefore SROs cannot be held liable for the actions of their members.

2.4 Are there requirements only at national level?

Yes, all requirements are adopted at national level. Constituent entities of the Russian Federation have no power to impose any requirements in this area.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

According to the Regulations of the Federal Financial Monitoring Service (Presidential Decree No. 808 dated 13 June 2012), the agency is authorised to inspect activities of legal entities as to their compliance with anti-money laundering requirements. According to the Federal Law "On the Central Bank of the Russian Federation (the Bank of Russia)" as part of its function to implement, with respect to credit and non-credit financial institutions and their officers, measures provided for by the Russian legislation for breaches of the requirements of Federal Law No. 115- FZ dated 1 August 2001 "On the Prevention of Criminal Proceeds Legalisation (Laundering) and Terrorist Financing", the Central Bank has authority to inspect activities of certain organisations. All the requirements that must be adhered to by legal entities and individuals are imposed by public legislative acts.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Federal Financial Monitoring Service and the Financial Monitoring and Currency Control Department of the Central Bank of Russia collect and analyse information on compliance with anti-money laundering requirements.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The statute of limitations for money laundering is 10 years from the date an offence was committed. The statute of limitations for breaching anti-money laundering requirements is one year from the date an offence was committed. The statute of limitations for an administrative offence in this sphere is six years.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Any breach of anti-money laundering requirements is an administrative offence subject to a fine imposed on officers in the amount ranging from 30,000 to 50,000 roubles and on legal entitles – in the amount ranging from 500,000 to 1,000,000 roubles.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Depending on the person committing an offence, as well as monetary fines, the following penalties are imposed: with respect to officers – disqualification for a period between one and three years; and with respect to legal entities – suspension of activities for up to 90 days.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Russian criminal law does not currently impose criminal liability for

non-compliance with requirements of anti-money laundering legislation. Legal entities, their officer and natural person might be held administratively liable for non-compliance with AML laws and requirements.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The relevant public agency, within the scope of its authority, collects information about an offence, allows the potential offender a right to offer explanations and issues a decision in administrative matters. Such decisions can be challenged in a court of law. They are not usually published but they are not secret, whereas a court decision would normally be published on the court's website. Financial institutions often challenge resolutions imposing fines on them, sometimes successfully and sometimes not.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Any organisation conducting operations with monetary funds or property are subject to the applicable anti-laundering requirements in Russia. For the purposes of this Federal Law, organisations conducting operations with monetary funds or other property include:

- credit organisations;
- securities market professionals;
- insurance organisations (with the exception of medical insurance organisations operating exclusively in the field of compulsory medical insurance), insurance brokers and leasing companies;
- federal postal services;
- pawn shops;
- organisations buying and selling precious metals and precious stones, jewelry made of them and scrap of such products, save for religious organisations, museums and organisations using precious metals, their chemical compounds, precious stones for medical, research or as part of tools, instruments, equipment and products for industrial purposes;
- organisations keeping betting and gambling shops as well as companies organising lotteries, *pari mutuel* and other risk-based activities, including through electronic means;
- management companies of investment funds, mutual funds and non-state pension funds;
- organisations that provide intermediary services in the implementation of transactions of purchase and sale of real estate;
- payment operators;
- commercial organisations entering into financing agreements under the assignment of a monetary claim as financial agents;
- consumer credit cooperatives, including agricultural credit consumer cooperatives;
- microfinance organisations;
- mutual insurance companies;
- non-state pension funds in terms of the implementation of non-state pension provision activities; and
- communication operators having the right to independently provide mobile radio telephone communication services, as well as communication operators occupying a significant position in the public telecommunications network, who have the right to independently provide communication services for data transmission.

The rights and obligations imposed by this Federal Law on organisations engaged in operations with monetary funds or other property are extended to individual entrepreneurs who are insurance brokers, individual entrepreneurs engaged in buying and selling precious metals and precious stones, jewelry made of them and scrap of such products, and individual entrepreneurs who provide intermediary services in the implementation of transactions of purchase and sale of real estate.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

As of today, the cryptocurrency industry is not subject to anti-money laundering requirements. However, introduction of amendments to the applicable legislation that would include companies trading cryptocurrency have been initiated by the Federal Service for Financial Monitoring (*Rosfinmonitoring*) and are now under development by the State Duma committee.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

The only legislative requirement is that each organisation puts in place an anti-corruption programme. The general approach is that a legal entity should comply with all AML requirements no matter how this goal is achieved. In case the legal entity (or its officers) fails to comply with such regulations, the legal entity will be held liable.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

As a general rule, a transaction involving cash and other property is subject to mandatory controls if the amount of such transaction is equal to, or larger than, 600,000 roubles or is equal to the amount in foreign currency equivalent to 600,000 roubles. A report on such transaction must be submitted to the competent agency no later than the day after the transaction takes place.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There are no notification requirements with respect to transactions not exceeding 600,000 roubles.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

International payment transfers are subject to control where the transfer amount exceeds 100,000 roubles. A bank must notify the competent agency within the first 20 days of the month following the month in which the transaction in question took place.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

An organisation carrying out transaction that is subject to control must identify the client as well as their representative, i.e. it must establish the identity and the documents on the basis of which the representative is acting on behalf of their client.

For foreign customers it is necessary to collect complete information on the organisation, such as registration codes, jurisdiction (country), competent agency, representative, etc.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

As a general rule, these transactions are subject to mandatory control if they involve a transfer of funds, receipt or grant of loan, a securities transaction, and in which at least one party is an individual or a legal entity registered, residing or having presence in a territory (state) which does not comply with the recommendations by the Financial Action Task Force (on Money Laundering) (FATF), or if such transactions are carried out through an account opened with a bank registered in such territory (state).

3.9 What is the criteria for reporting suspicious activity?

Information on transaction of an amount exceeding 600,000 roubles must be communicated to a competent agency, as well as information on suspicious transactions of smaller amounts. Criteria for suspicious activity are established by the bank carrying out the financial transaction in question.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The government maintains a register of legal entities that contains information about their management and owners. All changes (such as change of a CEO or share owners) are effective after they are registered.

A legal entity must know its beneficial owners and take measures (that are reasonable and available in the circumstances) to obtain their identification information. Banks are entitled to request information on beneficial owners of their customers.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

A payment order must contain accurate information on the payer and payee (names and taxpayer identification numbers). The bank will reject any payment order without such information.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

The legislation does not currently allow for the issuance of bearer shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes. The Federal Law "On the Prevention of Criminal Proceeds Legalisation (Laundering) and Terrorist Financing" also imposes requirements on the following non-credit organisations: leasing companies; payment processors; organisations acting as intermediaries in transactions for the sale and purchase of real estate; sole traders acting as intermediaries in transactions for the sale and purchase of real estate; and commercial organisations entering into factoring agreements as financial agents.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Such requirements apply to organisations listed in question 3.1 above.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Work is currently being carried out to create a single database of untrustworthy clients. Certain measures for identifying beneficial owners of offshore companies are also being strengthened.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

Overall, no there are not.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

A system of combatting financial terrorism in the Russian Federation has been recognised as fully compliant with the international standards. The Financial Action Task Force (FATF) has removed Russia out of the list of countries subject to closer monitoring aimed at identifying shortcomings in the anti-money laundering legislation.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Each statute is published in the official issue of Parlamentskaya Gazeta, Rossiyskaya Gazeta, or the Collection of Laws of the Russian Federation. Databases of such legislative acts are also widely available.

Rustam Kurmaev
Rustam Kurmaev and Partners
Capital City Complex, North Block
Moscow-City Business Centre
8, Presnenskaya nab., Bldg. 1
Moscow, 123100
Russia

Tel: +7 495 150 0505
Email: rustam.kurmaev@rkplaw.ru
URL: www.rkplaw.ru/en

Rustam Kurmaev is one of the toughest dispute resolution lawyers on the Russian market. He is known for his expertise in the criminal defence of business and legal support for companies in disputes with governmental authorities, including law enforcement agencies, and is a highly-regarded expert on issues involving the observance of anticorruption legislation (compliance). Rustam Kurmaev was the winner of the Client Choice Awards 2015–2016 in the nominating category "Russian Litigation", and also the winner of the 2015 Global Corporate Livewire Awards in the category "Anti-Corruption and Compliance". He is listed as a top-recommended attorney in the area of corporate compliance and investigation according to the *Global Investigation Review 100* for 2015. The international legal directory *Best Lawyers* in Russia has from 2012 through to 2019 consistently included Rustam Kurmaev on its list of the best Russian lawyers in the field of litigation, based on the consensus of the legal community of his peers.

Dmitry Gorbunov
Rustam Kurmaev and Partners
Capital City Complex, North Block
Moscow-City Business Centre
8, Presnenskaya nab., Bldg. 1
Moscow, 123100
Russia

Tel: +7 495 150 0505
Email: dmitry.gorbunov@rkplaw.ru
URL: www.rkplaw.ru/en

Dmitry Gorbunov heads the white-collar criminal defence practice at Rustam Kurmaev and Partners. He specialises in representing client interests in the litigation of cases involving corporate conflicts, business disputes, hostile takeovers and the criminal defence of business. He boasts a wealth of experience representing client interests at the commercial courts and courts of general jurisdiction at all levels and instances, as well as positive experience in the resolution of disputes with administrative bodies, including in cases involving administrative offences.

Rustam Kurmaev and Partners was established in October 2017 as an independent dispute resolution practice with a particular focus on commercial litigation, corporate conflict, white-collar crime, disputes with regulators and state authorities, and criminal defence of businesses in Russia. RKP also have significant background in representing clients in bankruptcy proceedings, complex insurance disputes, and high-value construction disputes. The firm is a spinoff of the Russian practice of a major global law firm. It was launched to be able to offer clients a tailored approach to solving the most complex legal issues they are facing without the additional bureaucratic burden of a large firm, while maintaining competitive rates and boasting a high level of partner involvement. A creative approach to problem-solving, a results-based management strategy, always striving to achieve excellence and offer top-notch legal advice to the clients – these are the team's core values and the underlining principles of their work.

Singapore

Lee Bik Wei

Lee May Ling

Allen & Gledhill LLP

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The Attorney-General ("**AG**"), as the Public Prosecutor ("**PP**"), has the legal authority to prosecute money laundering ("**ML**") in Singapore.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) ("**CDSA**") criminalises the laundering of proceeds generated by drug dealing/criminal conduct:

- assisting another person in retaining, controlling or using the benefits of drug dealing/criminal conduct under an arrangement (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise) (Section 43(1)/44(1));
- concealing, converting, transferring or removing from the jurisdiction, or acquiring, possessing or using property that represents a person's own benefits of drug dealing/criminal conduct (Section 46(1)/47(1));
- concealing, converting, transferring or removing from the jurisdiction property that represents another person's benefits of drug dealing/criminal conduct (Section 46(2)/47(2));
- acquiring, possessing or using property that represents another person's benefits of drug dealing/criminal conduct (Section 46(3)/47(3)); and
- possessing or using any property that may be reasonably suspected to be benefits from drug dealing/criminal conduct, if the person fails to account satisfactorily for how the person came by the property (Section 47AA(1)).

What must be proven

Physical elements:

The PP must prove that the accused carried out the relevant physical act of the said offence. Under Section 43(1)/44(1), this means that the PP must prove that (i) the accused entered into or is concerned in an arrangement, (ii) which facilitated another person in retaining, controlling or using the benefits of drug dealing/criminal conduct, and (iii) that other person is a person who engages in drug dealing/criminal conduct.

Under Sections 43, 44, 46, 47, the PP must also prove that the property was the benefits of drug dealing or criminal conduct; whereas under Section 47AA, the PP must only prove that the property would be suspected by a reasonable person of being benefits from drug dealing/criminal conduct.

Mental/fault element: Strict liability is imposed under Sections 46(1)/47(1).

Under Section 47AA(1), the accused must give a satisfactory explanation for how he came by the property. This section was introduced to combat ML operations involving money mules.

As for the other ML offences, the PP must prove that the accused knew or had reasonable grounds to believe that:

- (i) the arrangement would facilitate the retention, control or use of another person's benefits of drug dealing/criminal conduct, and (ii) the other person is a person who engages in drug dealing/criminal conduct or has benefitted from drug dealing/criminal conduct (Section 43(1)/44(1)); and/or
- the property represents another person's proceeds of crime.

Predicate offences

Predicate offences are listed in the First and Second Schedules of the CDSA, and include the conspiracy, attempt, abetment or incitement of another to commit such offences. The First Schedule identifies a "drug dealing offence" (which includes the ML offences under Sections 46 and 47). The Second Schedule identifies a "serious offence" constituting criminal conduct.

Predicate offences also include foreign drug dealing or serious offences, i.e. an offence against the law of a foreign country which would also constitute an offence listed in the First or Second Schedules of the CDSA, if the conduct had occurred in Singapore (Section 2(1) CDSA).

Whether tax evasion is a predicate offence for money laundering

Yes. Tax evasion under Sections 96 and 96A of the Singapore Income Tax Act (Cap. 134) and the national law of a foreign country (based on specific proscribed conduct) is a predicate offence for ML (Second Schedule and Section 2(1) CDSA).

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The CDSA has extraterritorial application as it applies to properties (including money and all other forms of property) in Singapore or elsewhere (Section 3(5) CDSA), and foreign drug dealing/serious offences (see question 1.2 above).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Commercial Affairs Department ("**CAD**"), a specialist department within the Singapore Police Force, is the principal law enforcement agency for the criminal investigation of ML offences. The Corrupt Practices Investigation Bureau or the Central Narcotics Bureau may also be involved.

The Attorney-General's Chambers is responsible for prosecuting ML offences.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is both corporate criminal liability and liability for natural persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Under Sections 43, 44, 46 and 47, the penalty is:

- for an individual, a fine not exceeding S$500,000, or imprisonment not exceeding 10 years, or both; and
- for a non-individual, a fine not exceeding the higher of S$1 million or twice the value of the benefits of drug dealing/criminal conduct in respect of which the offence was committed.

Under Section 47AA, the penalty is:

- for an individual, a fine not exceeding S$150,000, or imprisonment not exceeding three years, or both; and
- for a non-individual, a fine not exceeding S$300,000.

1.7 What is the statute of limitations for money laundering crimes?

There is no statute of limitations for the prosecution of ML crimes.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes. Singapore does not have state or provincial criminal offences.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

There is no separate forfeiture/confiscation authority. Upon conviction for one or more predicate offences in the CDSA, and on the PP's application, the Court may make a confiscation order against the defendant in respect of benefits derived by him or her from drug dealing/criminal conduct if the Court is satisfied that such benefits have been so derived (Sections 4 and 5 CDSA).

A confiscation order compels the defendant to pay an amount assessed to be the value of the benefit derived by the defendant from drug dealing/criminal conduct (Section 10 CDSA). Confiscation orders operate as if they were a fine imposed by the Court. In default of payment, the defendant may be subject to imprisonment.

Material/financial gains from organised crime activity can be confiscated without the need for a criminal conviction under the Organised Crime Act 2015 (No. 26 of 2015) ("**OCA**"). A CO under the OCA is not dependent on and is not affected by any criminal proceedings, even if the accused is acquitted. Upon the PP's application, the Court will make a CO if the Court is satisfied, on a balance of probabilities, that the person has carried out an organised crime activity within the defined statutory period and has derived benefits from the organised crime activity.

"Organised crime activity" refers to any activity carried out by a person in (or outside) Singapore amounting to a serious offence specified in the Schedule to the OCA (which includes Sections 43, 44, 46 and 47 of the CDSA) and is carried out at the direction of/in furtherance of the illegal purpose of a group which the person knows or has reasonable grounds to believe is an (locally-linked) organised criminal group (Section 48(1)(a)–(b) OCA).

It also includes activity amounting to an offence under Part 2 of the OCA (Section 48(1)(c) OCA). Part 2 of the OCA contains a group of provisions that criminalise being a member of an organised criminal group, instructing or facilitating the commission of an offence by such a group, and recruiting of members and expending of property to support these groups.

"Property" is defined in the same way as the CDSA (Section 2(1) OCA).

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Directors, officers or employees of regulated financial institutions ("**FIs**") have been convicted in Court for ML offences. One example is Yeo Jiawei, a former wealth planner at BSI Bank Limited, who was sentenced to 54 months' imprisonment for ML and cheating in a case related to the Malaysian state fund 1Malaysia Development Berhad ("**1MDB**").

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions against a company, partnership or unincorporated association may be resolved through the use of a Deferred Prosecution Arrangement ("**DPA**") (Part VIIA of the Criminal Procedure Code (Cap. 65A)). The DPA is an agreement between the PP and entities facing potential prosecution for certain specified criminal offences (including the MLs offences at question 1.2). A DPA comes into force only when the High Court approves it and declares that the DPA is in the interests of justice, and its terms are fair, reasonable, and proportionate. After such approval, the PP must give public notice of the DPA and the High Court's declaration and reasoning.

It is not applicable to individuals.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The Monetary Authority of Singapore ("**MAS**") investigates alleged

breaches of anti-money laundering ("**AML**") requirements on FIs in Singapore.

Other authorities that impose AML requirements on non-financial businesses and professions ("**Designated Businesses**") include:

- the Casino Regulatory Authority of Singapore (for casinos);
- the Accounting and Corporate Regulatory Authority ("**ACRA**") (for corporate service providers, public accountants and accounting entities); and
- the Council for Estate Agents (for estate agents and salespersons).

For more details of these requirements, see section 3 below.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes. These include the Institute of Singapore Chartered Accountants (for professional accountants) and the Law Society of Singapore (for law practices and legal practitioners).

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, they may have their own enforcement measures against members. For example, legal practitioners and law practices are subject to AML requirements under the Legal Profession Act (Cap. 161) (including the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015), and a breach of these rules may subject the legal practitioner to disciplinary proceedings and/or the law practice to regulatory action.

2.4 Are there requirements only at national level?

Yes, Singapore does not have different levels.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

MAS is responsible for ensuring compliance and enforcement of AML requirements under MAS-administered laws and regulations. MAS's enforcement approach is outlined in the Enforcement Monograph, which is available on the MAS website. MAS guidelines in respect of what constitutes compliance with AML requirements are also publicly available on its website.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Suspicious Transaction Reporting Office ("**STRO**") is Singapore's FIU. The STRO is the central agency for receiving, analysing, and disseminating suspicious transaction reports ("**STR**"), Cash Transaction Reports ("**CTR**") and Physical Currency and Bearer Negotiable Instruments ("**CBNI**") Reports ("**CBNIR**").

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitations for enforcement actions.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

These vary across industries.

Under Section 27B(2) of the MAS Act (Cap. 186), a FI that fails to comply with any AML direction issued or regulation made by MAS is liable to a fine not exceeding S$1,000,000, and in the case of a continuing offence, is also subject to a further fine of S$100,000 for every day or part of a day during which the offence continues after conviction.

MAS may, in its discretion, compound any offence which is punishable with a fine only by collecting from a person reasonably suspected of having committed the offence a sum not exceeding one half of the amount of the maximum fine prescribed for that offence (Section 176(1) MAS Act). On payment of such sum, no further proceedings shall be taken against that person in respect of that offence.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

These vary across industries.

For FIs, MAS can impose non-financial sanctions such as:

- revocation or suspension of regulatory status (e.g. BSI Bank Limited and Falcon Private Bank Ltd, Singapore Branch in relation to 1MDB);
- removals of directors and officers;
- prohibition orders ("**PO**") barring persons from conducting regulatory activities or from taking part in management of the FI (e.g. MAS has issued POs against numerous individuals in relation to 1MDB);
- reprimands; and
- warnings.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, violations of AML obligations may also be subject to criminal sanctions.

For FIs, failing to comply with its AML obligations is an offence (Section 27B(2) MAS Act) (see question 2.8). MAS may also refer matters to the CAD to evaluate whether criminal offences have been committed.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The relevant regulatory authority will assess the appropriate sanction(s) to be imposed based on its own guidelines and

precedents. It is possible but rare to apply for judicial review of administrative decisions. An individual issued with a PO may appeal to the Minister in charge of MAS.

Typically, most resolutions of penalty actions are published by the relevant regulatory authority. MAS publishes enforcement actions against FIs and individuals on its website.

As penalty assessments are usually composition fines, FIs do not challenge such composition fines.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

FIs include:

- banks;
- merchant banks;
- finance companies;
- money changers;
- remittance agents;
- insurers;
- insurance brokers;
- capital markets intermediaries;
- trust companies;
- financial advisers;
- The Central Depository (Pte) Ltd (the Depository); and
- stored value facility holders.

Designated Businesses include:

- casino operators;
- corporate service providers;
- dealers in precious stones and/or precious metals ("**PSMD**");
- estate agents and salespersons;
- legal practitioners and law practices;
- moneylenders;
- pawnbrokers; and
- professional accountants and professional accounting firms (including public accountants and accounting entities).

The applicable AML obligations are set out in specific statutes, subsidiary legislation, directions, guidelines, codes, and practice notes/circulars. Broadly, they require FIs or Designated Business to implement procedures that cover the following important areas:

- risk assessment and risk mitigation, and applying a risk-based approach;
- undertaking customer due diligence ("**CDD**") measures;
- recordkeeping requirements;
- STR requirements; and
- developing and implementing internal policies, procedures, and controls.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Parliament passed the Payment Services Act (No. 2 of 2019) ("**PSA**") on 14 January 2019, which will come into operation on a date appointed by the Minister. Under the PSA, a person carrying on a business of providing any service of dealing in digital payment tokens or any service of facilitating the exchange of digital payment tokens will have to meet AML/countering the financing of terrorism ("**CFT**") requirements, to be imposed on relevant licensees through MAS Notices.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

FIs and Designated Businesses must implement a compliance framework commensurate with their risk profile and the nature, scale and complexity of their business. This typically includes measures in relation to risk assessment and mitigation, CDD, reporting, recordkeeping, and internal policies, procedures, and controls, including ongoing monitoring of business dealings with customers (see question 3.1). Further details are in the sections below.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Recordkeeping

FIs and other Designated Businesses must retain CDD information and other data, documents and information relating to a transaction for at least five years. This may include details of its risk assessments, information on business relations with or transactions for a customer, and information pertaining to a matter that has been the subject of an STR.

FIs must retain records of financial transactions for a minimum of five years (Section 37 CDSA).

PSMDs must also maintain records of cash transactions exceeding S$20,000, as well as customer information, for a period of five years (Section 48I of CDSA). On 11 February 2019, Parliament passed the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 ("**PSPMA**"), which will come into operation on a date appointed by the Minister. The PSPMA establishes a more comprehensive supervisory and regulatory regime for a "regulated dealer" (which will include dealing in asset-backed tokens and intermediaries) to strengthen AML/CFT safeguards.

Reporting large currency transactions

A PSMD (or regulated dealer) must submit a CTR in respect of any cash transaction (or designated transaction), the aggregate of which exceeds S$20,000 in a transaction (or in a day) within the prescribed time (i.e. 15 days for PSMD under the CDSA). Any PSMD (or regulated dealer) who fails to comply with the above requirement shall be guilty of an offence and liable on conviction to a fine of up to S$20,000 and/or imprisonment up to two years. (Section 48J CDSA and Section 17 PSPMA).

A casino operator is required to file a CTR with the STRO for cash transactions with a patron (or on its behalf) involving an aggregate amount of S$10,000 or more in a transaction (or in any gaming, before the end of the applicable reporting period). Any casino operator which fails to comply with the above requirement shall be guilty of an offence and shall be liable on conviction to a fine not exceeding S$20,000.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Yes. STRs and CBNIRs are other type of reports that are filed with the STRO.

For when a STR must be filed, see question 3.9. For when a CBNI Report must be filed, see question 3.6.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes. A person who moves into or out of Singapore CBNI exceeding S$20,000 (or its equivalent in a foreign currency) must make a CBNIR in respect of the movement. A person who receives CBNI the total value of which exceeds S$20,000 (or its equivalent in a foreign currency) from outside Singapore must make a CBNI Report in respect of the receipt within five business days (Sections 48C and 48E CDSA, and regulations 2A and 4A, Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) Regulations 2007).

Certain limited exemptions are set out in Sections 48C(7) and 48C(8) of the CDSA and the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) (Exemption) Orders 2007 and 2010.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

These include:

(a) identifying and verifying the identity of the customer (or any beneficial owner in relation to the customer);

(b) understanding the purpose and intended nature of the business relationship with the customer; and

(c) ongoing monitoring of the business relationship with the customer.

A risk-based approach is commonly adopted. Enhanced CDD measures are required for politically exposed persons (entrusted with prominent public functions) or their family members or close associates, or if business relations with or transactions for a customer presents a higher risk of money laundering. Such circumstances include (but are not limited to) where the customer or beneficial owner is from or in a country or jurisdiction in relation to which the Financial Action Task Force ("**FATF**") has identified as being high-risk or which is known for having inadequate AML measures.

Enhanced CDD measures include obtaining the approval of senior management to establish or continue business relations with the customer, taking appropriate and reasonable measures to establish the customer's source of wealth and funds, and conducting enhanced ongoing monitoring of business relations with the customer.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes, FIs are prohibited from the following relationships with foreign shell banks:

- banks, finance companies and merchant banks: entering into or continuing correspondent banking or other similar services relationship (MAS Notice 626);
- capital markets intermediaries: correspondent account services relationship (MAS Notice SFA04-N02);
- money-changing or remittance business licensees: provision of remittance services (see MAS Notice 3001);
- CDP: correspondent account relations (MAS Notice SFA03AA-N01); and
- stored value facility holders: correspondent account services or other similar services relationship (MAS Notice PSOA-N02).

Each of the aforementioned FIs must also take appropriate measures when establishing the relevant relationship to satisfy itself that respondent FIs do not permit their accounts to be used by foreign shell banks.

3.9 What is the criteria for reporting suspicious activity?

Section 39 of the CDSA provides that a person must lodge a STR with the STRO if:

(a) he knows or has reasonable grounds to suspect that any property:

(i) in whole or in part, directly or indirectly, represents the proceeds of;

(ii) was used in connection with; or

(iii) is intended to be used in connection with, any act which may constitute drug dealing/criminal conduct; or

(b) the information or matter on which the knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment.

The STR must be made as soon as is reasonably practicable after it comes to the person's attention.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Generally, all businesses must register with ACRA. ACRA maintains this database of business entities (e.g. companies, sole proprietorships, partnerships) in Singapore and requires that the information in relation to the said entities be kept updated. Business information includes particulars of management, shareholders, secretaries, registered address, date of registration of the entity, date of change of name and/or address, issued and paid-up share capital, as well as charges held over assets of the entity (if any). Such business profiles of entities are publicly available online for purchase.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes. Information includes the wire transfer originator's name, account number or unique transaction reference number, unique identification number, and address, date/place of birth or incorporation or registration, and the wire transfer beneficiary's name and account number or unique transaction reference number.

These requirements do not apply to a transfer and settlement between the relevant FI and another FI where both FIs are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary (see paragraph 11 of MAS Notice 626, MAS Notice 824, and MAS Notice 1014, and paragraph 12 of MAS Notice 3001).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No (see Sections 66 and 364 of the Companies Act (Cap. 50)).

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes (see question 3.1).

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

The regulatory requirements are targeted at specific industries (see question 3.1). Industries such as banks, merchants and finance companies may engage in trade finance activities. In this regard, MAS issued a Guidance Paper on AML/CFT Controls in Trade Finance and Correspondent Banking in October 2015. The objective of the paper was to provide banks, merchant banks and finance companies with guidance on the AML/CFT controls in trade finance and correspondent banking, and to share sound practices intended to help banks strengthen their controls and risk management in relation to their trade finance activities.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

For the real estate sector in Singapore, Parliament passed the Developers (Anti-Money Laundering and Terrorism Financing) Act 2018 on 20 November 2018, which will come into operation on a date appointed by the Minister. Under this Act, property developers licensed under the Housing Developers (Control and Licensing) Act (Cap. 130) and the Sale of Commercial Properties Act will also be subject to similar AML requirements as discussed in question 3.1. This is part of government efforts to prevent the real estate industry from being used to facilitate the movement of illicit funds.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

No. In the last FATF and Asia/Pacific Group ("**APG**") on Money Laundering review published in September 2016, Singapore was assessed to have either a moderate or substantial rating for effectiveness and technical compliance with 10 out of 11 immediate outcomes, and a low rating in respect of the immediate outcome for terrorism-financing investigation and prosecution. Singapore was also assessed to have either a compliant or largely compliant rating in respect of 34 out of a total of 40 recommendations, and a partially compliant rating in respect of the remaining six recommendations.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The most recent evaluation was jointly conducted by the FATF and APG from 18 November to 4 December 2015. Results were published in September 2016, as mentioned in question 4.2.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The relevant AML laws, regulations, administrative decisions, and guidance can be obtained from various official websites. These include Singapore Statutes Online (http://sso.agc.gov.sg/) and MAS's website (http://www.mas.gov.sg).

Lee Bik Wei
Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7825
Email: lee.bikwei@allenandgledhill.com
URL: www.allenandgledhill.com

Bik Wei is the Deputy Head of the Firm's White Collar & Investigations Practice. Her other main areas of practice include civil and commercial litigation and arbitration.

She advises multinational corporations, private and listed companies, and trust companies, and has experience in a wide range of areas including contractual disputes, shareholder disputes, corporate governance matters such as breach of directors' duties, employment, investigations, property and trust, and restructuring and insolvency.

Bik Wei is also proficient in Mandarin and has advised Chinese clients in arbitral proceedings. She joined the Firm in 2008 and has been with the Firm since.

Lee May Ling
Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7823
Email: lee.mayling@allenandgledhill.com
URL: www.allenandgledhill.com

May Ling is a Senior Associate in the Firm's White Collar & Investigations Practice. Her key areas of practice are in corporate & commercial disputes and white-collar crime & investigations. She has acted in a wide range of matters for multinational corporations, corporate trustees and private and publicly-listed entities.

May Ling advises companies on putting in place and managing whistleblowing and dawn raid policies and procedures. She also regularly acts for companies who are conducting internal investigations and/or are involved in investigations by enforcement authorities such as the Commercial Affairs Department, Corrupt Practices Investigation Bureau and the Monetary Authority of Singapore. This includes situations where the investigations develop into criminal prosecutions by the Attorney General's Chambers.

May Ling graduated from King's College London with an LL.B. (First Class Honours) degree in 2009. She pursued an LL.M. (Commercial Law) in King's College London the following year before returning to Singapore and getting called to the Singapore Bar in 2012.

ALLEN & GLEDHILL

Allen & Gledhill is an award-winning full-service South-east Asian commercial law firm which provides legal services to a wide range of premier clients, including local and multinational corporations and financial institutions. Established in 1902, the Firm is consistently ranked as one of the market leaders in Singapore and South-east Asia, having been involved in a number of challenging, complex and significant deals, many of which are first of its kind. The Firm's reputation for high-quality advice is regularly affirmed by the strong rankings in leading publications, and by the various awards and accolades it has received from independent commentators and clients. The Firm is consistently ranked band one in the highest number of practice areas, and is one of the firms with the highest number of lawyers recognised as leading individuals. Over the years, the Firm has also been named 'Regional Law Firm of the Year' and 'SE Asia Law Firm of the Year' by many prominent legal awards. With a growing network of associate firms and offices, Allen & Gledhill is well-placed to advise clients on their business interests in Singapore and beyond, in particular, on matters involving South-east Asia and the Asia region. With its offices in Singapore and Myanmar; its associate firm, Rahmat Lim & Partners in Malaysia; and its alliance firm, Soemadipradja & Taher in Indonesia, the Allen & Gledhill network has over 550 lawyers in the region, making it one of the largest law firms in South-east Asia.

Switzerland

Omar Abo Youssef

Kellerhals Carrard

Lea Ruckstuhl

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

In accordance with art. 305*bis* no. 1 of the Swiss Criminal Code (SCC), any person who carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or from a qualified tax offence, shall be punishable by imprisonment of up to three years or a monetary penalty.

The criminal offences under art. 186 of the Federal Act on Direct Federal Tax and art. 59 para. 1 first lemma of the Federal Act on the Harmonization of Direct Taxes of the Cantons and Municipalities shall be deemed to be qualified tax offences if the evaded taxes exceed CHF 300,000 per tax period. The crucial point in this instance is that, for the purpose of tax evasion, falsified, forged or substantively untrue documents are used for fraudulent purposes.

According to the Federal Supreme Court, and regardless of the clear wording of art. 305*bis* no. 1 SCC, the actions described as "frustrating the identification of the origin and the tracing of assets" shall not have any independent significance in comparison to "frustrating the forfeiture".

The perpetrator of the predicate offence can also be punished for subsequent money laundering.

Money laundering is only punishable if it has been committed with direct or conditional intent.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Under Swiss law, the crime of money laundering pursuant to art. 305*bis* SCC protects the criminal authorities' right to forfeiture. Thus, in order to establish money laundering the criminal authority has to prove:

(i) that a predicate offence (felony or qualified tax offence) has been committed;

(ii) that assets originating from such predicate offence could be forfeited;

(iii) that the offender intentionally committed an act aimed at frustrating the forfeiture of such assets; and

(iv) that the offender knew or should have known that the assets originate from a predicate offence.

Generally speaking, money laundering applies to felonies, i.e. criminal offences that are punished with a prison sentence of more than three years, and to qualified tax offences.

Consequently, predicate offences include, *inter alia*, the most important offences against property (e.g. misappropriation [art. 138 SCC], theft [art. 139 SCC], robbery [art. 140 SCC], fraud [art. 146 SCC], criminal mismanagement [art. 158 SCC], handling stolen goods [art. 160 SCC]), bankruptcy offences (art. 163 *et seq.* SCC), certain forms of drug dealing (art. 19 para. 2 of the Federal Act on Narcotics and Psychotropic Substances), bribery (art. 322*ter et seq.* SCC), including bribery of foreign public officials (art. 322*septies* SCC).

As for taxes, the evasion of *indirect* taxes (customs duties, withholding tax, stamp duties, VAT, etc.) is punished with a prison sentence up to five years and thus anyway qualifies as a felony and predicate offence to money laundering, provided the conditions of art. 14 para. 4 Federal Act on Administrative Criminal Law are fulfilled, that is if it:

(i) is committed commercially or in cooperation with third parties; and

(ii) causes a significant unlawful advantage or a significant damage to public authorities.

The evasion of *direct* taxes, on the other hand, does not qualify as a felony under Swiss law. However, since the beginning of 2016 money laundering still applies to so-called qualified tax offences relating to direct taxes (*cf.* question 1.1 above).

Among Swiss law experts there is a dispute as to whether the new offence of money laundering in tax matters is indeed functional since avoidance of taxes in principle (i) triggers no forfeiture, but just a supplementary tax assessment, and (ii) does not lead to the acquisition of specific assets which originate from the qualified tax offence and could be forfeited.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

If the predicate offence, in other words the felony or the qualified tax offence, was committed abroad and is punishable there, then the perpetrator shall be prosecuted and punished in Switzerland for the money laundering committed in Switzerland (art. 305*bis* no. 3 SCC). This provision serves to protect the foreign forfeiture claim. Applying the provision to foreign predicate offences can therefore be problematic if a foreign state does not know the concept of

forfeiture of specific (tainted) assets, but rather absorbs tortious benefits exclusively by means of a claim for compensation (see also question 1.9 in this regard).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Depending on whether the money laundering is directed against the Federation's or the Canton's administration of justice, criminal proceedings for money laundering are conducted either by the Federal Prosecutor's Office or by the cantonal public prosecutor's offices (art. 23 para. 1 *lit.* h of the Swiss Code of Criminal Procedure [SCP]). If money laundering is, to a large extent, carried out abroad or in several cantons without being concentrated in one canton, then the Federal Prosecutor's Office shall be responsible for prosecution (art. 24 para. 1 SCP). However, under certain conditions the Federal Prosecutor's Office can transfer a criminal case that falls under its jurisdiction in accordance with art. 23 SCP to the cantonal prosecutor's offices for investigation (art. 25 SCP).

The Money Laundering Reporting Office Switzerland (MROS) similarly plays an important role in the prosecution of money laundering. It receives reports from financial intermediaries who transmit them by virtue of their reporting rights or their reporting obligation, and subsequently reviews and analyses them (see question 2.6). It notifies the relevant prosecuting authority if it has reason to suspect that money laundering has taken place or that assets originate from a felony or a qualified tax offence in accordance with art. 305*bis* no. 1*bis* SCC.

Any violations of the reporting obligation (art. 37 of the Federal Act on Combating Money Laundering and Terrorist Financing [AMLA]) are prosecuted by the Federal Department of Finance (art. 50 para. 1 of the Federal Act on the Swiss Financial Market Supervisory Authority [FINMASA]). For more details about the reporting obligation, please see question 3.9.

1.5 Is there corporate criminal liability or only liability for natural persons?

In Switzerland, both natural persons and companies can be prosecuted and convicted for money laundering. In accordance with art. 102 para. 1 SCC, any felony or misdemeanour committed in a company in the exercise of commercial activities in accordance with the objects of the company is attributed to the company if that act cannot be attributed to any specific natural person due to inadequate organisation of the company (subsidiary corporate liability).

In accordance with art. 102 para. 2 SCC, the company shall be punished independently or in addition to the criminal liability of any natural persons if the felony or misdemeanour involves certain offences, including in particular money laundering, and if the company has failed to take all the reasonable organisational measures in order to prevent such an offence (cumulative corporate liability).

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

In the event of natural persons being convicted in accordance with art. 305*bis* no. 1 SCC, the maximum prison sentence is three years. In qualified cases (art. 305*bis* no. 2 SCC), in particular, if the perpetrator is acting as a member of a criminal organisation or as a member of a group that has been formed for the purpose of the continued conduct of money laundering activities, or if he/she achieves, by means of commercial money laundering, a large turnover or a substantial profit, then the maximum prison sentence shall be five years, combined with a maximum monetary penalty of 500 daily penalty units of up to CHF 3,000 each.

If a company is convicted of money laundering, the maximum fine shall be CHF 5 million (art. 102 para. 2 in conjunction with para. 1 SCC).

1.7 What is the statute of limitations for money laundering crimes?

The limitation period for prosecution is 10 years (art. 97 para. 1 *lit.* c SCC) for the basic offence of money laundering (art. 305*bis* no. 1 SCC) and 15 years (art. 97 para. 1 *lit.* b SCC) for the qualified offence (art. 305*bis* no. 2 SCC). As money laundering is an ongoing offence, the limitation period for prosecution begins on the day on which the criminal conduct ceases (art. 98 *lit.* c SCC). The limitation period for prosecution ceases to apply if a judgment by a court of first instance has been issued before the limitation period for prosecution has expired (art. 97 para. 3 SCC).

It should be noted that the limitation period for prosecution of the predicate offence also plays a role. If the predicate offence is barred by a statute of limitation, then no forfeiture or money laundering in terms of frustrating the forfeiture will be possible. The limitation period for prosecution of predicate offences (felonies and qualified tax offences) is 15 years.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

There are no money laundering provisions in Switzerland on a cantonal or municipal level. Only art. 305*bis* SCC applies. However, criminal proceedings for money laundering are also prosecuted by the cantonal prosecutors (see question 1.4).

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

In accordance with art. 70 para. 1 SCC, the court orders the forfeiture of assets that have been acquired through the commission of a criminal offence, unless the assets are passed on to the person harmed for the purpose of restoring the prior lawful position.

Forfeiture shall only be precluded if a third party has acquired the assets in ignorance of the grounds for forfeiture and has (cumulatively) provided an equivalent consideration for them or if forfeiture would otherwise cause him disproportionate hardship (art. 70 para. 2 SCC).

The objects of forfeiture are assets obtained directly or indirectly by means of a criminal offence. These must have a natural and adequate causal link to the criminal offence, but do not necessarily have to be the direct and immediate consequence of the offence. For example, income from legal transactions that have been concluded based on bribery can also be confiscated. It is undisputed that surrogates of assets acquired through a criminal offence can be confiscated as well.

If the assets which are subject to forfeiture no longer exist, e.g., because they have been consumed or disposed of, then the court orders a compensation claim for the same amount (art. 71 para. 1

SCC). The compensation claim may be enforced in any assets, including assets which may have been legally acquired. Frustrating the compensation claim does not qualify as money laundering since it does not focus on "tainted" assets. Money laundering applies only to frustrating the forfeiture of "tainted" assets that are proven to be directly or indirectly derived from a felony or a qualified tax offence.

It is an issue of controversy whether the scope of the benefit to be recovered should be determined on a net or gross basis. For generally prohibited activities (e.g., drug trafficking), gross calculations apply, whereas for acts that are permitted in principle, but are only tortious in specific instances (e.g., a contract that has been obtained through corrupt means), net calculations are used, i.e. the production costs are deducted.

Law enforcement authorities may order the provisional seizure of assets if they are likely to be forfeited or serve to enforce the compensation claim (art. 263 para. 1 *lit.* d SCP, art. 71 para. 3 SCC).

As forfeiture and compensation claims involve objective measures and not penalties, these sanctions are applied regardless of the criminal liability or conviction of a particular person. This is on the condition, however, that all objective and subjective elements of the underlying offence can be proven and that there is no general defence.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes. It is worth mentioning, for example, the conviction of bank officers for money laundering by omission (BGE 136 IV 188). The relevant case was based on the following facts: the bribes received by tax officials from the District of Rio de Janeiro were transferred to accounts of a bank headquartered in Geneva. Although the question of the admissibility of a PEP engaging in secondary employment did relate to one of the officials, internal transfers to other tax officials did take place, and the accounts showed a rapid increase in capital, the evidence thus suggested that the tax officials' balances could be of criminal origin; the bank officers neglected to inform the bank's general management. As a result of this omission, they breached the duties of care incumbent on them and prevented the accounts from being reported to MROS and being blocked.

Another ruling of the Federal Supreme Court relates to the criminal liability of a bank for lack of organisational measures to prevent money laundering (BGE 142 IV 333). The decision was based on the following facts: After the transfer of EUR 5 million to an account at the bank – the transfer was based on fraud – the amount of CHF 4.6 million was withdrawn in cash. The Federal Supreme Court denied the bank's cumulative liability for money laundering since the necessary conditions, i.e. the underlying criminal liability of a natural person for money laundering, was not established. The case shows that the cumulative liability of companies for money laundering is indeed cumulative and not strict liability.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Plea agreements as known, e.g., in the U.S. are not known in Switzerland. However, criminal prosecution may be abandoned in certain circumstances, in particular if the offender has made reparations (art. 53 SCC). In this regard, reference should be made to the abandoning of corruption proceedings against a French company on the basis of art. 53 SCC, after it had made reparations to the value of CHF 1 million. At the same time, however, the Swiss subsidiary of the same concern was sentenced, by means of a summary penalty order, to a fine of CHF 2.5 million as well as a claim for compensation to the value of CHF 36.4 million.

In accordance with Federal Supreme Court case law, orders for abandoning prosecutions can be inspected if there is a legitimate interest in the information and it is not opposed by any overriding public or private interests.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The basic principles for combatting money laundering are laid down in the Federal Act on Combating Money Laundering and Terrorist Financing (AMLA). The scope of application of the AMLA as well as the duties for the traders are clarified in the Anti-Money Laundering Ordinance of the Federal Council.

The obligations for the prudentially supervised financial intermediaries (especially banks) and those for the Swiss Financial Market Supervisory Authority FINMA subordinated financial intermediaries (DSFIs) are specified in the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA). The duties of the financial intermediaries affiliated with the self-regulatory organisations are regulated in the corresponding self-regulatory organisation's statutes. Depending on the financial intermediary, supervision is carried out by the FINMA, the self-regulatory organisations, the Federal Gaming Board, or the supervisory commission of the Swiss Bankers Association's for its Code of Conduct with regard to the exercise of due diligence (CDB) (see questions 2.2 and 2.3). Reference is hereby made to questions 3.1 and 3.7 for the requirements related to combatting money laundering.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

If the financial intermediaries pursuant to art. 2 para 3 AMLA do not submit themselves directly to FINMA supervision, they must join a recognised self-regulatory organisation and the regulations of this self-regulatory organisation shall apply. It should be mentioned that the prudentially supervised banking sector has established a Code of Conduct with regard to the exercise of due diligence with FINMA's agreement. The Code of Conduct applies to the identification of the customer and establishing the identity of the beneficial owner of the assets involved in the business relationship or the transaction. It should also be emphasised that the statutes for self-regulatory organisations for the Swiss Insurance Association for Combating Money Laundering (SRO SVV) govern the due diligence obligations for all insurance institutions, even if they have not been subject to the supervision of the SRO SVV.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes. In accordance with art. 12 lit. c AMLA, supervising compliance with the due diligence obligations of the financial

intermediaries mentioned in art. 2 para. 3 AMLA is the responsibility of the self-regulatory organisations recognised by FINMA, unless the financial intermediaries have directly submitted themselves to the supervision of FINMA. FINMA, in turn, actively monitors the self-regulatory organisations.

2.4 Are there requirements only at national level?

Yes, requirements are only at national level.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

FINMA is responsible for monitoring FINMA's direct and prudentially supervised financial intermediaries (especially the banks). The self-regulatory organisations are responsible for enforcing the requirements *vis-à-vis* their affiliated financial intermediaries. It should be emphasised that the banks, in addition to FINMA, are also supervised by their professional organisation's supervisory committee.

FINMA publishes the procedure in connection with auditing in the context of circulars, as well as various information on so-called "enforcement proceedings".

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Money Laundering Reporting Office Switzerland (MROS) at the Federal Office of Police is the national central office which examines suspicious transaction reports, analyses them and, if necessary, forwards them to the relevant law enforcement authorities.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

By virtue of art. 52 FINMASA, the prosecution of any violations of this law and of the financial market laws has a limitation period for prosecutions of seven years.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Self-regulatory organisations do not have a homogeneous fine policy and the fines vary in terms of amount. The Swiss Bankers Association's Supervisory Commission may, for example, issue penalties of up to CHF 10 million. The offences that can lead to fines or penalties are specified in the corresponding regulations. FINMA itself does not have any authority to issue fines.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

Violating the due diligence obligations of the AMLA may call into question the "guarantee of proper business conduct" demanded by the financial intermediary. If FINMA detects a serious violation of supervisory provisions, it may, in accordance with art. 33 FINMASA, prohibit the person responsible from acting in a management capacity towards any person or entity subject to its supervision. The prohibition from practising a profession may be imposed for a period of up to five years.

Authorisation to exercise financial intermediary activity may be withdrawn from companies. In addition, FINMA may, by virtue of art. 35 FINMASA, confiscate any profit that a supervised person or entity or a responsible person in a management position has made through a serious violation of the supervisory provisions.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

If the reporting obligation specified in art. 9 AMLA is violated, then natural persons can be prosecuted in accordance with art. 37 AMLA (intentional violation: fines of up to CHF 500,000; negligence: fines of up to CHF 150,000).

Furthermore, a natural person can be punished for money laundering under art. 305*bis* SCC, although the grounds for this offence can also be met by omission (imprisonment for up to three years or a fine, in severe cases imprisonment for up to five years). In addition, there is a specific offence for the financial intermediaries which fail to determine the identity of the beneficial owner of the assets with the due diligence required by the circumstances (art. 305*ter* para. 1 SCC, imprisonment for up to one year or a fine).

In addition, art. 102 para. 2 SCC is to be mentioned, which, in the context of a money laundering offence, stipulates that the company will also be punished if it has not taken all necessary and reasonable organisational measures to prevent an offence of this nature (see question 1.5).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

As a rule, FINMA does not comment on individual enforcement proceedings. Cases of particular regulatory interest are exceptions to this rule. Many self-regulatory organisations do not make decisions on penalties public. There are in some cases reports in which information is provided in a summarised and anonymised form on the practice of penalties. Financial intermediaries have already challenged decisions on penalties.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The AMLA and the due diligence obligations that it contains apply, on the one hand, to financial intermediaries (art. 2 para. 2 and 3 AMLA) and, on the other hand, to traders (art. 2 para. 1 lit. b

AMLA), who receive more than CHF 100,000 in cash. The term financial intermediaries specifically includes banks, insurance companies, fund management companies and investment companies (the latter both under certain conditions), securities dealers and casinos. In addition, persons are also considered to be financial intermediaries if they professionally lend, provide payment services, or manage assets.

Please refer to question 3.7 for a description of the due diligence obligations.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The Swiss Financial Market Supervisory Authority FINMA assesses the Money Laundering risks as especially high in a decentralised blockchain-based system, where assets can be transferred anonymously and without regulated intermediaries.

In February 2018, FINMA published guidelines regarding Initial Coin Offerings (ICOs). Based on these guidelines, FINMA focuses on the economic function and purpose of the token issued by the ICO organiser. Relevant is the underlying purpose of the token and if they are tradeable or transferable. FINMA distinguishes between payment tokens, utility tokens and asset tokens. If the ICO issues already existing payment tokens, it is qualified as a means of payment and subjected to the AMLA. Either the ICO organiser affiliates itself to an SRO or is licensed directly by the FINMA and fulfils the AMLA-obligations itself (e.g. identifying the contracting party) or these requirements can be fulfilled – exceptionally – through "delegation", by having the funds accepted via a financial intermediary, which is already subject to the AMLA and who exercises the corresponding customer due diligences for the ICO organiser.

The ICO of utility tokens or asset tokens are not qualified as means of payment under the AMLA and therefore not subjected to the AMLA.

Under current FINMA practice, the exchange of a cryptocurrency for fiat money or a different cryptocurrency falls under art. 2 para. 3 AMLA. The custodian wallet provider, the online exchange office and the centralised trading platform are subject to the AMLA as well.

Furthermore it has to be noted that in September 2018, the Swiss Bankers Association published guidelines for its members regarding opening corporate accounts for blockchain companies.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

AMLO-FINMA sets specific requirements for certain types of financial intermediaries. Art. 20 para. 2 AMLO-FINMA should be mentioned, for example, which stipulates that banks and securities dealers must operate a computer-based system for monitoring transactions. Such system will help to identify transactions with increased risks.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

All documents required in connection with the fulfilment of the due diligence obligations must be kept for 10 years after the business relationship in question has been terminated or the transaction has been carried out (art. 7 para. 3 AMLA). There is no obligation, however, to automatically report large currency transactions.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

There are at present no automatic reporting requirements in Switzerland for any transactions.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There is no obligation to automatically report cross-border transactions.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

1) Identifying the contracting party: A financial intermediary must identify the contracting party on the basis of a valid document (e.g. passport or extract from the commercial register) when commencing a business relationship.
2) Establishing the identity of the beneficial owner of the assets: In the case of natural persons, the financial intermediary must determine whether there are any doubts about the principle that the contracting party is also the beneficial owner of the assets. Since 01/01/2016, financial intermediaries must also identify the controlling person of legal entities. The controlling person is always a natural person.
3) Repetition of the verification of the identity of the customer or the establishment of the identity of the beneficial owner in the event of doubt.
4) Special duties of due diligence: The financial intermediary shall also be required to identify the nature and purpose of the business relationship that the contracting party wishes to establish. The scope of the information to be obtained depends on the (money laundering) risk represented by the contractual partner or the planned business relationship or transaction (referred to as "risk-based approach"). In addition, the contractual partner must be investigated for (but not exclusively) his/her status as a politically exposed person, but also for any matches on sanction and terrorist lists.
5) Documentation and retention obligations: Documentation must be created concerning the transaction carried out and concerning the clarification required in accordance with the AMLA and be retained for at least 10 years after the business relationship has come to an end.
6) Organisational measures: These include the sufficient training of staff and internal in-house controls. AMLO-FINMA specifically requires the establishment of an anti-money laundering department that monitors compliance with the anti-money laundering laws and carries out random checks, issues instructions, plans and monitors internal AML-training and makes the necessary reports to the Money Laundering Reporting Office.
7) Obligations in the event of suspected money laundering: In the event of a reasonable suspicion of money laundering or

terrorist financing, the financial intermediary must provide a report to the Money Laundering Reporting Office and, if necessary, take further measures (e.g. an asset freeze and information ban).

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

In accordance with art. 8 lit. b AMLO-FINMA, the financial intermediary may not start any business relationships with banks of this nature unless they are part of a consolidated group of financial institutions that is appropriately monitored in a consolidated fashion.

3.9 What is the criteria for reporting suspicious activity?

A financial intermediary must immediately notify the Money Laundering Reporting Office if it knows, or has reasonable grounds to suspect, that the assets involved in the business relationship are related to a criminal offence under art. 260*ter* number 1 (criminal organisation) or art. 305*bis* SCC (money laundering), are the proceeds of a felony or a qualified tax offence, are subject to the power of disposal of a criminal organisation or serve the financing of terrorism (art. 260*quinquies* para. 1 SCC). Furthermore, the financial intermediary shall have a duty to report if it cancels negotiations for commencing a business relationship based on a reasonable suspicion of this nature. Finally, the financial intermediary shall also be required to report if the financial intermediary, in accordance with the provisions of art. 6 para. 2 lit. d AMLA knows or has reason to believe that the data forwarded by FINMA, the Federal Gaming Board or a self-regulatory organisation concerning the so-called terrorist lists correspond to the data of the customer, a beneficial owner or the authorised signatory of a business relationship or transaction.

In addition, the financial intermediaries shall be entitled to report any observations to MROS that suggest assets are the result of a felony or a qualified tax offence (art. 305*ter* para. 2 SCC).

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Currently there is no publicly accessible register that contains information about the beneficial owners of an operating legal entity who ultimately control the legal entity. However, there is a commercial obligation to keep a register of bearer shareholders and beneficial owners of the bearer and nominal shares.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes. Based on art. 10 of the AMLO-FINMA, the payer's financial intermediary for the payment order must state the name, the account number, and the address of the payer as well as the beneficiary's name and the account number. There are certain easements for payment orders within Switzerland.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Bearer shares are not prohibited in Switzerland. However, there are efforts to abolish the bearer shares. Furthermore, the acquisition must be reported within one month, by providing personal details and identifying the bearer shareholder. In addition, the beneficial owner of the shares must be notified if the limit of 25% of the share or voting interest is reached or exceeded. If the shareholder has not met its reporting obligations, then its membership rights shall be suspended. Furthermore, its property rights will be forfeited if the notification is not made within one month of the acquisition having taken place. If the bearer shareholder collects the notification at a later date, it may only assert the property rights arising from that date.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No. However, if a trader carries out a transaction of CHF 100,000 in cash, it must then comply with the limited due diligence and reporting obligations under art. 17 *et seq.* of the Anti-Money Laundering Ordinance of the Federal Council.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

No, there are not.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Due to the fact that Switzerland narrowly failed the FATF country evaluation in 2016 and is in the so-called enhanced follow-up, a duty on the part of the financial intermediary to verify the customer's information on the beneficial owner and an event-independent obligation for the regular updating of the customer documentation shall be introduced. In addition, discussions are underway to lower the threshold for the reporting obligation, so that the financial intermediaries will, in future, have to report in the event of mere simple suspicion on the basis of art. 9 AMLA. In June 2018, the Federal Council of Switzerland published a legislative draft amending the AMLA. The scope of the AMLA should be extended and due diligence obligations are to be introduced for certain services which concern the establishment, management or administration of companies and trusts (except operating companies in Switzerland). This amendment especially focuses on lawyers and notaries and will apply the AMLA duties (in amended form) as well to them. Furthermore, associations which are at risk of being misused for terrorism or money laundering must be entered in the commercial register. When these legislative amendments will enter into force and what will be the final wording of the legislative text is not yet clear.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

See question 4.3.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

On 7 December 2016, the fourth FATF Country Report for Switzerland was published. Switzerland scored well for the legal mechanisms. Switzerland was rated as "compliant" or "largely compliant" for 31 of the 40 recommendations. With regard to the effectiveness of the legal provisions, Switzerland scored high in seven out of the 11 subject areas examined. Switzerland achieved above-average results in comparison to the other countries that have already been audited.

However, this does not change the fact that Switzerland did fail the country evaluation, like many other countries. This is especially the case because, according to the FATF, Switzerland's efforts in connection with establishing the identity of the beneficial owner and especially with verifying this information have been insufficient to date. There is, therefore, a need for action in the area of technical compliance, in other words primarily at the level of the AMLA and the regulations and rules issued by the SRO. It is expected that a duty to verify the information on the beneficial owner as well as a regular and event-independent obligation to update customer information will be introduced. The relevant revisions are under consideration or already in progress (see question 4.1 above).

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

We refer to the following links:

- Federal Department of Foreign Affairs FDFA – Fighting money laundering and terrorist financing: https://www.eda.admin.ch/eda/en/home/foreign-policy/financial-centre-economy/fighting-international-crime.html.
- Money Laundering Reporting Office Switzerland (MROS): https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html.
- Swiss Criminal Code, SCC (*cf.* in particular art. 70 *et seq.* and art. 305*bis* SCC): https://www.admin.ch/opc/en/classified-compilation/1937 0083/index.html.
- Anti-Money Laundering Act, AMLA: https://www.admin.ch/opc/en/classified-compilation/1997 0427/index.html.

Acknowledgment

The authors would like to acknowledge Florian Baumann, Responsible Partner, for his contribution to this chapter. Florian is head of the Kellerhals Carrard White Collar Crime practice group and represents clients in multinational asset recovery cases, criminal and administrative legal assistance proceedings and internal investigations. He advises banks and other financial intermediaries on compliance issues, including representation in administrative investigations or compliance-related litigation.

Omar Abo Youssef

Kellerhals Carrard
Rämistrasse 5
PO Box, 8024 Zürich
Switzerland

Tel: *+41 58 200 39 00*
Email: *omar.aboyoussef@kellerhals-carrard.ch*
URL: *www.kellerhals-carrard.ch*

Omar Abo Youssef is a member of Kellerhals Carrard's White Collar Crime practice group. He graduated from the University of Zurich (Juris Doctor and Master of Law) and Geneva (Certificate of Transnational Law) and is admitted to all Swiss courts. He lectures in criminal law and criminal procedural law at the University of Zurich. Omar Abo Youssef specialises in complex criminal, regulatory and civil litigation matters, with a special focus on white-collar crime, the prevention of money laundering and international assistance in criminal matters. Omar Abo Youssef has authored numerous publications on matters of criminal law, criminal procedural law, international criminal law and international assistance in criminal matters, including the chapters on tax offences and enforcement of criminal judgments in the Basel Commentaries on Swiss tax law and on International Criminal Law.

Lea Ruckstuhl

Kellerhals Carrard
Rämistrasse 5
PO Box, 8024 Zürich
Switzerland

Tel: *+41 58 200 39 00*
Email: *lea.ruckstuhl@kellerhals-carrard.ch*
URL: *www.kellerhals-carrard.ch*

In 2007, Lea Ruckstuhl completed a Master of Law at the University of Freiburg with the addition of European law ("*summa cum laude*") and received the Frilex Prize for the best university degree. She was admitted to the Bar in 2010 and has been with Kellerhals Carrard since 2011.

As head of the department of the self-regulatory organisation for the Swiss Leasing Association (SRO/SLV), she has broad experience in the field of leasing and financing. Her main areas of practice include financial market supervision (non-banks and insurance companies), in particular in the field of combatting money laundering, as well as general contract law, commercial law and company law. She is also a member of the Audit and Investigation Body of the self-regulatory organisation of the Swiss Insurance Association and a member of the Board of Directors of the Association Forum SRO. Lea Ruckstuhl is co-author of the in 2017 published book about Compliance.

Kellerhals Carrard

With more 200 professionals (comprised of partners, salaried lawyers, legal experts, tax advisers and notaries) and a total of more than 300 staff, the law firm Kellerhals Carrard, which dates back to 1885 and has offices in Basel, Berne, Geneva, Lausanne, Lugano, Sion and Zurich and representation offices in Binningen, Shanghai and Tokyo, is the second largest in Switzerland and boasts a rich tradition.

Kellerhals Carrard operates throughout Switzerland, whilst maintaining very strong local roots, advising clients nationally and abroad. The firm advises and represents companies and entrepreneurs from all industries and economic sectors, public authorities, national and international organisations and private individuals before all judicial and administrative bodies nationally and abroad in practically all areas of the law.

In recent years, governments have increased their efforts and adapted their laws and regulations in order to fight fraud, corruption, money laundering, financing of criminal activities and terrorism. As a result, criminal law is increasingly important for international business and finance.

Over the years, Kellerhals Carrard has developed a substantial practice in the field of national and transnational commercial criminal law. The firm's attorneys have also been closely involved in developments in this field through their lecturing activities and publications. Kellerhals Carrard's Investigation, Compliance and White Collar Crime team consists of 27 lawyers.

United Arab Emirates

AlShamsi Lawyers & Legal Consultants

Hamdan AlShamsi

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The legal authority that prosecutes any person is the General Public Persecutor.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The law criminalises as money laundering any of the following acts carried out in the knowledge that the funds are derived from a crime:

- the conversion, transfer, deposit, safekeeping, investment, exchange or management of any proceeds of crime, with intent to conceal or disguise the illicit origin thereof;
- the concealment or disguise of the true nature, origin, location, way of disposition, movement or rights related to any proceeds or the ownership thereof; or
- the acquisition, possession or use of such proceeds.

These acts are only considered money laundering when the perpetrator is aware that the funds in question are derived from illicit sources. Therefore money laundering is always an intentional act and may not be committed by negligence.

Money laundering is independent of the predicate crime and the punishment of the person who has committed a predicate offence shall not prevent him or her from being punished for money laundering.

Tax evasion is not included as an offence for money laundering in the UAE laws.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The general rule is that any monies that have been laundered in the UAE which originated from a crime committed in a foreign jurisdiction are punishable; however, the UAE law provides for exceptions to this rule. One of the important exceptions is that the same crime must be punishable in the UAE as well. There are also other rules in this respect and these are circumstantial.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The following government entities are involved in the enforcement and regulation of the UAE's AML regime:

- the UAE Central Bank;
- the National Anti-Money Laundering Committee (NAMLC);
- the UAE's Anti-Money Laundering and Suspicious Cases Unit (AMLSCU);
- the Emirates Securities and Commodities Authority (SCA);
- the Insurance Authority (IA);
- the Dubai Financial Services Authority (DFSA) of the Dubai International Financial Centre Free Zone (DIFC); and
- the Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market Free Zone (ADGM).

The various governing rules of the above-listed regulatory bodies provide them with powers to conduct periodic and *ad hoc* assessments of regulated persons.

On a local level, Dubai Law No. 4 of 2016 established the Dubai Economic Security Centre (DESC), which is empowered to regulate the economic and financial activity of entities based both onshore and in Dubai's free zones in order to combat financial crimes including money laundering.

As to the prosecution of money laundering criminal offences, this remains under the authority of the General Public Persecutor.

1.5 Is there corporate criminal liability or only liability for natural persons?

The AML laws and regulations issued by the UAE authorities impose various restrictions on financial and other institutions. Any non-compliance with a set of duties imposed may constitute a breach of the AML laws or regulations. The AML Law explicitly denotes three separate instances where individuals or companies would be considered to have violated AML duties. These instances are as follows:

- There is an obligation on employees of any institution in the UAE to report money laundering, terrorism and terrorist funding activities to the AMLSCU; the financial intelligence unit of the Central Bank. Failure to disclose knowledge of such activities to the relevant authorities can lead to penalties including imprisonment, fines or both.
- Furthermore, some articles criminalise 'tipping-off' entities to ongoing investigations and provide for penalties of imprisonment or a fine.

Other articles criminalise intentional failure to report or disclose information that is requested by the authorities during AML investigations.

There are additional relevant regulations that apply to declarations by travellers entering or leaving the UAE carrying cash or monetary financial bearer instruments.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

If convicted of a money laundering offence, the AML Law provides punitive measures including fines ranging from 10,000 to 1 million dirhams and imprisonment for up to 10 years.

1.7 What is the statute of limitations for money laundering crimes?

The general statute of limitations for criminal offences is five years, however, such limitation starts from the time that the authorities discover any money laundering activities and not from the date of the money laundering activities.

1.8 Is enforcement only at the national level? Are there parallel state or provincial criminal offences?

The enforcement is at a national level and there are no state criminal offences other than what is mentioned above where in specific emirates they carry their own criminal offences for similar acts or acts connected to the AML Law.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The AML Law provides for the forfeiture of the proceeds of money laundering offences, as well as the property, equipment and tools used or intended to be used in the commission of the offence. Additionally, some articles mandate that the court must confiscate any items connected with any criminal offence and, in cases where no items are seized, the court must order a fine of the equivalent value.

As mentioned above, in the case of an accusation, the public prosecutor must issue a freezing order against any property or assets connected to an offence of money laundering.

Any civil forfeiture will not be made through the AML Law, rather a civil claimant must claim and prove his claim to receive any of his funds. In the case of other nations, they may request that the UAE freeze and transfer any seized property that has been found as a result of the money laundering.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Answer not available at time of going to press.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The AML Law does not provide a method by which to settle a money laundering offence and therefore such facts and terms may not be public. However, if the crime from which the monies were laundered for any reason was to be settled and therefore the monies would cease to be derived from a crime, then in such a circumstance there can be a reason for the AML articles not to apply.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

In cases where compliance standards have not been met, administrative sanctions are available to ensure proper application of the law. Such measures include: warnings; fines; restriction or suspension, or both, of business activity; cancellation of licence; and restricting the power of the board and senior management, facilitated by the appointment of a temporary observer.

If convicted of a money laundering offence, the AML Law provides punitive measures including fines ranging from 10,000 to 1 million dirhams and imprisonment for up to 10 years.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

No, there are not.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

No, other than to ensure that their members are not convicted of any Anti-Money Laundering crimes.

2.4 Are there requirements only at national level?

No, they are not.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

These agencies are the same agencies mentioned above in question 1.1.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements? If so, are the criteria for examination publicly available?

Yes, the UAE's Central Bank FIU is the government's Financial Intelligence Unit.

The criteria for examination are included in the following details:

The AML Law is supported by implementing resolutions and other regulations and guidance issued by relevant supervisory bodies that encourage the use of a risk-based approach when on-boarding customers and conducting periodic AML assessments during the course of the business relationship.

The UAE's AML/CTF framework has adopted international best practices laid out by the Financial Action Task Force (FATF) and follows FATF guidance on high-risk areas. For instance, the UAE Central Bank Circular No. 3701/2012 refers to FATF documents that analyse jurisdictions according to their AML/CTF deficiencies and advise financial institutions to apply relevant countermeasures suitable to the jurisdiction's AML/CTF competency.

Other high-risk areas include identifying the beneficial owners and forming a business relationship with an FPEP. Opening bank accounts for FPEPs generally requires prior written approval by the Central Bank.

Dealers in precious metals, real estate and other luxury goods, non-resident account holders and other cash-intensive businesses are also considered high risk and require stringent due diligence procedures.

AML regulations and guidance emphasise the necessity of continuous AML/CTF risk appraisal. Enhanced due diligence is required in cases where there is cause for suspicion, such as changed business relationships, one-off or complex transactions, transactions with no apparent economic justification or the observance of other red flags. Where relevant, reporting is an essential part of law enforcement.

Compliance with AML regulations is mandatory and must be accompanied by thorough supporting documentation.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The statute of limitations is five years, as mentioned above.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

As mentioned above in question 2.1, the AML Law carries penalties including fines and a high possibility of imprisonment. The regulatory authorities (as applicable) may stop the institutions from working or other possible measures in case of money laundering.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The legal entities and individuals can be stopped from continuing their current activities by the authorities.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

Yes, anti-money laundering obligations are subject to criminal sanctions.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process varies from one authority to another and the penalty actions are seldom public. Financial institutions and persons can challenge administrative penalties with the authority and such a challenge varies from one department to another. Any persons convicted of an AML crime at the judiciary can challenge the judgment by way of an appeal to the Supreme/Cassation courts.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

Financial institutions regulated by the UAE Central Bank are required to carry out AML measures in accordance with Central Bank circulars. Circulars also provide detailed guidance on other critical issues, such as foreign politically exposed persons (FPEP) and customer accounts. These are issued from time to time to reflect global AML activity.

Markets, companies and institutions licensed by the SCA are required to comply with SCA Decision (17/R) of 2010 concerning 'Anti-money laundering and terrorism finance combating procedures'.

Regulated entities in the UAE free zones are also required to comply with rules provided by relevant regulatory bodies. For regulated persons in the DIFC, this relates to the Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module of the DFSA Rulebook (the AML Module) and the Anti-Money Laundering and Sanctions Rules and Guidance of the FSRA (the AML Rulebook) for those in the ADGM.

Designated Non-Financial Businesses and Persons (DNFBPs) are covered by additional relevant laws and regulations. DNFBPs include: lawyers, public notaries and other legal professionals; accountants, auditors and auditing firms; real estate agents; and dealers of gold, jewellery and precious metals.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

There are no amendments to the Anti-Money Laundering regimes that have incorporated any new articles in respect to the cryptocurrency industry, however, the same principles found in the Anti-money laundering laws will apply as well to the cryptocurrency industry.

In June 2018, Abu Dhabi Global Market (ADGM), the International Financial Centre in Abu Dhabi, launched its framework to regulate spot crypto asset activities, including those undertaken by exchanges, custodians and other intermediaries in ADGM. Other regulators in the country, namely the central bank of the UAE and the DIFC, have not yet issued a law that regulates cryptocurrencies.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

As per the Central Bank regulations, all banks and other financial institutions are required to appoint an employee as the 'compliance officer'.

The compliance officer is responsible for:

- liaising with and contacting the Central Bank to report money laundering and suspected cases and sending reports;
- training other members of staff;
- receiving calls and contacts regarding AML compliance;
- ensuring that internal control systems operate efficiently; and
- ensuring that money laundering and terrorist financing risks are mitigated and controlled.

In addition, banks and other financial institutions should ensure:

- compliance officers are appointed based on competency, subject to a 'fit and proper' test before employment;
- the compliance officer's function is subject to independent audit review by the internal audit department and regular reports are submitted to the chief executive; and
- all compliance-related staff are given periodic training and more frequent in-house courses on handling AML and CTF cases.

For DFSA-regulated entities, appointing compliance officers and specifically a money laundering reporting officer (MLRO) is mandatory as per the DFSA Rulebook. Regulated entities may also outsource the function of the MLRO, based on the test of competency.

The MLRO is responsible for overseeing the AML function of the regulated entity, incorporating responsibilities of training staff, submitting STRs and responding to queries from relevant authorities.

Entities regulated by the FSRA are subject to similar obligations.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

The AML Regulations specifies that all institutions shall maintain records for a period of five years from the following:

- the date of the closure of accounts of clients;
- the date on which the transaction took place in the absence of an account;
- the culmination of a regulatory inspection by a regulatory authority; or
- the date of issuance of a final judgment by a relevant judicial authority.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

As previously mentioned, the AML Law mandates that employees of any institution in the UAE must report money laundering, terrorism and terrorist funding activities to the AMLSCU. Failure in this duty can lead to penalties, including imprisonment, fines or both.

Correspondingly, articles within the law criminalises the intentional failure to report or disclose information that is requested by the authorities during AML investigations.

The same law states that any individuals or entities that report suspicious transactions will be exempt from any resultant administrative, civil or criminal penalties, provided that the reporting is done in good faith.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes, the institutions who are handling such transaction must report the origin and destination of the transaction, the amount, the purpose of the transaction, and any available information related to that transaction.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

On 14 December 2016, the UAE Central Bank issued a resolution to amend Circular No. 24/2000 concerning Procedures for Anti-Money Laundering and its amendments, modernising its identification procedures in order to strengthen its anti-money laundering regulations. The Resolution altered the phraseology of the existing Circular to expand customer identification requirements and provide that banks must now personally inspect either the original UAE identity card or the passport of any individual opening a new bank account, whereas before it covered only passports. This prevents the opening of fraudulent bank accounts under assumed names or numbers. The Resolution is reflective of the Central Bank's commitment to complying with the Recommendations for the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation published by the FATF in October 2016.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

As per the Dubai Financial Services Authority "DFSA" Rulebook Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML) A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

Rule 6.1.3 prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank. The DFSA does not consider that the existence of a local agent or low-level staff constitutes physical presence.

Rule 9.2.2 prohibits an Authorised Firm from entering into a correspondent banking relationship with a Shell Bank or a bank which is known to permit its accounts to be used by Shell Banks. See the Guidance after Rule 6.1.4 for more information about what constitutes a Shell Bank.

An Authorised Firm must:

(a) not enter into a correspondent banking relationship with a Shell Bank; and

(b) take appropriate measures to ensure that it does not enter into, or continue a corresponding banking relationship with, a bank which is known to permit its accounts to be used by Shell Banks.

For the purposes of these Rules, a Relevant Person means:

(a) an Authorised Firm other than a Credit Rating Agency;

(b) an Authorised Market Institution;

(c) a DNFBP; or

(d) a Registered Auditor.

3.9 What is the criteria for reporting suspicious activity?

Money laundering and Terrorist Financing mean the criminal offences defined in the Federal AML legislation.

A Relevant Person must ensure that where the Relevant Person's MLRO receives a notification under Rule 13.2.2, the MLRO, without delay:

(a) inquires into and documents the circumstances in relation to which the notification made under Rule 13.2.2 was made;

(b) determines whether in accordance with Federal AML legislation a Suspicious Activity Report must be made to the AMLSCU and documents such determination;

(c) if required, makes a Suspicious Activity Report to the AMLSCU as soon as practicable; and

(d) notifies the DFSA of the making of such Suspicious Activity Report immediately following its submission to the AMLSCU.

Rule 13.3.2 states that where, following a notification to the MLRO under 13.2.2, no Suspicious Activity Report is made, a Relevant Person must record the reasons for not making a Suspicious Activity Report.

Rule 13.3.3 states that a Relevant Person must ensure that if the MLRO decides to make a Suspicious Activity Report, his decision is made independently and is not subject to the consent or approval of any other person.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

Yes, it is very prevalent in the UAE to request information regarding the beneficial owner to property and companies.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Yes, the institution must: (a) when it sends or receives funds by wire transfer on behalf of a customer, ensure that the wire transfer and any related messages contain accurate originator and beneficiary information; (b) ensure that, while the wire transfer is under its control, the information in (a) remains with the wire transfer and any related message throughout the payment chain; and (c) monitor wire transfers for the purpose of detecting those wire transfers that do not contain originator and beneficiary information and take appropriate measures to identify any money laundering risks.

The requirement set out above does not apply to an institution which transfers funds to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

The institution must ensure that information accompanying all wire transfers contains, at a minimum: (a) the name of the originator; (b) the originator account number where such an account is used to process the transaction; (c) the originator's address, or national identity number, or customer identification number, or date and place of birth; (d) the name of the beneficiary; and (e) the beneficiary account number where such an account is used to process the transaction.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Bearer shares are not available in the UAE. The company laws do not allow bearer shares.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the AML module has been designed to provide a single reference point for all persons and entities (collectively called Relevant Persons) who are supervised by the DFSA for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and sanctions compliance under the two regimes referred to above. Accordingly, it applies to Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions (DNFBPs), and Registered Auditors.

Recommendations set out in the issued Guidelines are not mandatory and it is up to each DNFBP to determine the extent to which they implement such recommendations. Each DNFBP is responsible for his own policies and implementation.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Criminal regulations and laws apply to all entities within the UAE but within the UAE some authorities will be responsible for certain persons and entities within different geographical areas. An example of that is that the DFSA covers the DIFC area whilst the central bank covers the whole of the UAE, except for the DIFC.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

Customer due diligence (CDD) requirements are specified by the AML Regulations, as well as various sector-specific regulations issued by the different governing bodies.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

No, there are not.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes, for example, there is an assessment of the anti-money laundering (AML) and combatting the financing of terrorism (CFT) regime of the United Arab Emirates (UAE) is based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT assessment Methodology 2004, as updated in February 2007. The assessment team considered all the materials supplied by the authorities, the information obtained on site during their mission from February 28 to March 15, 2007, and other verifiable information subsequently provided by the authorities. During the mission, the assessment team met with officials and representatives of all relevant government agencies and the private sector. A list of the bodies met is set out in Annex 1 to the detailed assessment report.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The materials are sometimes found online and the original language is Arabic. As for any DIFC related material, they can be found on the DFSA website.

Hamdan AlShamsi
Hamdan AlShamsi Lawyers
& Legal Consultants
Office 1611, 16th Floor, Al Manara Tower
Al Abraj Street, Business Bay
Dubai
UAE

Tel: +971 4 346 9262
Email: hamdan@alshamsilegal.com
URL: www.alshamsilegal.com

With nearly a decade of successful litigation experience across the United Arab Emirates, Mr. AlShamsi has built one of Dubai's most reputable and respected law practices. He is widely regarded as a top litigator in the Dubai Courts, with extensive experience in corporate, banking and finance and insurance law. Mr. AlShamsi advises both local and international companies and governmental entities in cases involving complex litigation. He appears regularly before the Appeals Court and the Court of Cassation, as well as UAE's Federal Supreme Court. Mr. AlShamsi has been described as being *"…very thorough and highly efficient – Hamdan faced each challenge with strategy, professionalism and confidence which ultimately resulted in our successful outcome"*. It is no surprise that he has been awarded as one of the most influential young leaders in the Middle East and the young achiever award, amongst many more.

HAMDAN ALSHAMSI
LAWYERS & LEGAL CONSULTANTS

Hamdan AlShamsi Lawyers & Legal Consultants was established in 2011. It has since become a name synonymous with success and is well-known in the legal circuit. The success of the law firm is due to its specialisation in advising on commercial issues, insurance, due diligence, family law, intellectual property law, banking, companies law and other matters locally, and its dedication towards offering unparalleled, high-quality and culturally sensitive legal services, while adhering to the highest standards of integrity and excellence.

United Kingdom

Mona Vaswani

Amy Edwards

Allen & Overy LLP

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

The United Kingdom (UK) money laundering offences are created by Part 7 of the Proceeds of Crime Act 2002 (**POCA**) and include:

- the principal money laundering offences; and
- the reporting offences which, with one exception, only apply to those operating in the "regulated sector".

It is also an offence under POCA to attempt, conspire, incite, aid, abet, counsel or procure the commission of a principal money laundering offence.

Note that there are similar offences relating to terrorist financing contained in the Terrorism Act 2000. The anti-terrorist financing regime in the UK runs parallel to the UK's anti-money laundering regime.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Principal money laundering offences

To establish that a principal money laundering offence has been committed, it is necessary to prove that:

(a) the alleged offender has:
  (i) concealed, disguised, converted or transferred criminal property; or removed criminal property from the jurisdiction; or
  (ii) entered into or become concerned in an arrangement which he knew or suspected facilitated the acquisition, retention, use or control of criminal property by or on behalf of another person; or
  (iii) acquired, used or had possession of criminal property; and

(b) the alleged offender:
  (i) failed to make an authorised disclosure and does not have a reasonable excuse for not making such a disclosure; or
  (ii) in relation to (a)(iii) above only, acquired, used or had possession of the property for adequate consideration.

For each of the principal money laundering offences, the conduct referred to in (a)(i), (ii) and (iii) above must concern "criminal property" and, as such, it must be established that:

(a) the relevant property constitutes a person's benefit from criminal conduct or represents such a benefit (whether in whole or in part, and whether directly or indirectly); and

(b) the alleged offender knew or suspected that the property represents such a benefit (this is a subjective limb).

The test for "criminal property" has an inbuilt assumption that there has been "criminal conduct" and, accordingly, there must be a predicate offence in order for criminal property to exist. Conduct which constitutes a criminal offence in any part of the UK is capable of forming a predicate offence for the purposes of money laundering.

Tax evasion constitutes a criminal offence under English law and, accordingly, is a predicate offence for money laundering. Further, the Criminal Finances Act 2017 introduced two new corporate failures to prevent the facilitation of tax evasion offences. These being criminal offences, they are also predicate offences for money laundering.

Reporting offences

Reporting offences include the failure to disclose, tipping-off and prejudicing a money laundering investigation.

To establish that a failure to disclose offence has been committed, broadly speaking, it is necessary to prove that:

(a) the alleged offender knew, suspected or had reasonable grounds for knowing or suspecting that another person is engaged in money laundering (this is an objective limb);

(b) the information or other matter on which that knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicious, came to him/her in the course of a business in the "regulated sector";

(c) the alleged offender can identify the person referred to in (a) above or the whereabouts of any laundered property, or he/she believes (or it is reasonable to expect him/her to believe) that the information or other matter referred to in (b) above will or may assist in identifying that person or the whereabouts of any laundered property (this is an objective limb); and

(d) the alleged offender failed to make the required disclosure and does not have a reasonable excuse for not making such a disclosure (or any other applicable defence).

To establish that the tipping-off offence has been committed it is necessary to prove that:

(a) the alleged offender has disclosed that:
  (i) a disclosure has been made by that person or another person under Part 7 of POCA in relation to information that came to that person in the course of a business in the regulated sector; or
  (ii) an investigation into allegations that an offence under Part 7 of POCA has been committed is being contemplated or carried out; and

(b) the disclosure is not a permitted disclosure, it is likely to prejudice an investigation, and the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

To establish the prejudicing of a money laundering investigation offence, it is necessary to prove that the alleged offender:

(a) knew or suspected that a person was acting in connection with a money laundering investigation which was being or was about to be conducted; and

(b) either knowingly;

(i) made a disclosure which was likely to prejudice that investigation; or

(ii) falsified, concealed, destroyed or otherwise disposed of, or caused or permitted the falsification, concealment, destruction or disposal of documents which are relevant to the investigation.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes, both the principal money laundering and the disclosure offences have extraterritorial application.

The definition of "criminal conduct" includes conduct which took place outside of the UK but which, had it occurred in any part of the UK, would constitute an offence under English law. Accordingly, provided that the other elements of the test are met, such conduct is capable of giving rise to "criminal property" for the purposes of the principal money laundering offences under POCA.

Further, the definition of "money laundering" includes an act which would constitute a principal money laundering offence had it been done in the UK. Therefore, provided that the other elements of the relevant offence are met, failure to disclose knowledge or suspicion (or where there were reasonable grounds for knowing or suspecting) that money laundering has taken/is taking place in another jurisdiction could give rise to a disclosure offence under POCA.

However, a person will not commit a principal money laundering offence if:

(a) he/she knew, or believed on reasonable grounds, that the relevant conduct occurred in a country or territory outside the UK; and

(b) the relevant conduct:

(i) was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory; and

(ii) does not constitute an offence punishable with imprisonment for a maximum term in excess of 12 months in any part of the UK if it had occurred there.

There are also similar overseas conduct defences in relation to the disclosure offences.

The Criminal Finances Act 2017 expanded the definition of "unlawful conduct" in Part 5 (civil recovery) POCA 2002 to include overseas conduct that constitutes (or is connected with) the commission of a gross human rights abuse or violation. Provided that the conduct, if it occurred in a part of the UK, would be unlawful under the criminal law of that part of the UK, there is no requirement for the conduct also to be unlawful overseas.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Money laundering offences are usually investigated by the National Crime Agency (**NCA**), the police or Her Majesty's Revenue and Customs (**HMRC**). As a rule, money laundering offences are prosecuted by the Crown Prosecution Service. However, there are exceptions to this, for example, cases involving serious fraud or corruption are likely to be investigated and prosecuted by the Serious Fraud Office and, as the financial services regulator, the Financial Conduct Authority (**FCA**) has the power to investigate and prosecute offences under POCA falling within its remit.

The National Economic Crime Centre (**NECC**) started operating on 31 October 2018. It is an overarching body to coordinate the UK's response to economic crime, including money laundering.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is corporate criminal liability for money laundering. Most of the offences in POCA apply to corporations as well as individuals. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) also create offences which apply to regulated firms (including banks and financial institutions). A regulated firm commits an offence under the MLR 2017 if it contravenes certain requirements relating to customer due diligence, policies and procedures, controls, and recordkeeping amongst other things.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Different offences under POCA have different maximum penalties. The highest maximum penalty is 14 years' imprisonment (for individuals) and/or an unlimited fine (applicable to both individuals and corporations).

An offence under MLR 2017 is punishable by up to two years' imprisonment (for individuals) and/or an unlimited fine (applicable to both individuals and corporations).

1.7 What is the statute of limitations for money laundering crimes?

There is no time limit in respect of which criminal conduct can give rise to criminal property, and accordingly, prosecutions can be brought at any time. However, offences under POCA cannot be committed retrospectively and money laundering offences committed before the commencement of POCA will be prosecuted under the previous legislation.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Broadly speaking, enforcement is at a national level. Part 7 of POCA (which, as noted above at question 1.1, contains the principal money laundering offences) applies equally throughout the UK, although there are separate (but similar) provisions for confiscation and restraint procedures in Scotland and Northern Ireland.

Note that the NCA's operational powers in Scotland are conditional on authorisation from the Lord Advocate.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The confiscation regime under POCA applies to offences committed

after 24 March 2003. A confiscation order deprives an individual – who has been convicted of a money laundering offence in the Crown Court – of the benefits of his proceeds of crime. Such orders may be granted at the request of the prosecution, or where the court deems it appropriate to do so.

Section 6 of POCA provides that the court can make a confiscation order in respect of any property unless it would be disproportionate within the meaning of Article 1 of the European Convention on Human Rights. This is a high threshold, and the court will not generally find that an order would be disproportionate unless it would clearly amount to double-counting. In 2017, the Court of Appeal found that a confiscation order which may result in the need to sell a jointly owned family home was not disproportionate.

Part 5 of POCA contains powers that enable an enforcement authority to pursue a civil recovery order, which facilitates the recovery of proceeds of crime without the need for a conviction. The court must be satisfied only that the property in question is or represents the proceeds of unlawful conduct. Section 13 of the Criminal Finances Act 2017 extends the definition (or meaning) of "unlawful conduct" to include conduct which occurs overseas but which constitutes, or is connected with, the commission of a gross human rights abuse or violation and which would be an offence triable under criminal law within the definition of unlawful conduct if it occurred in the UK. The main focus of the amendment is to help target the assets of foreign officials complicit in human rights abuses.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

We have not identified any cases in which financial institutions or their directors, officers or employees have been convicted of money laundering under POCA, the MLR 2017 or under the predecessor regulations which were in force from 2007 to 2017. All previous cases involve the imposition of civil penalties. The FCA had 75 open investigations into money laundering as at the publication of its last annual report. In July 2018, the Director of Enforcement and Market Oversight at the FCA stated that: "*We have also commenced a small number of investigations into firms' systems and controls where, for the first time, we have indicated to those firms that we are looking at whether there has been any misconduct that might justify a criminal prosecution under the Money Laundering Regulations.*"

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions are resolved through the judicial process. However, the FCA has wide powers to impose civil penalties and disciplinary sanctions on regulated firms for breach of the MLR 2017, and other regulations regarding AML systems and controls. These include unlimited fines, statements of public censure, and suspension and cancellation of regulatory permissions. In such cases, records of the fact and terms of settlements are usually public. Recent notable examples include:

(a) In July 2018 the FCA fined a bank GBP 896,000 and restricted it from accepted deposits for 147 days for failing to maintain effective AML systems and controls between 2012 and 2016.

(b) In January 2017, the FCA fined a bank GBP 163 million for failing to maintain an adequate AML framework between 2012 and 2015.

(c) In October 2016, the FCA fined a bank GBP 3.25 million for failing to maintain adequate AML systems and controls between 2010 and 2014, and prohibited the bank from accepting deposits from any new customers for 168 days. The bank's money laundering reporting officer was also fined GBP 17,900 and was prohibited from performing compliance oversight functions.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The principal AML requirements are contained in the MLR 2017. The MLR 2017 require relevant persons to, among other things, carry out appropriate levels of risk assessment, implement adequate policies, controls and procedures, and carry out appropriate levels of customer due diligence (**CDD**).

The FCA Handbook also requires firms to establish and maintain effective systems and controls for countering financial crime risk. Firms also need to consider guidance published by the Joint Money Laundering Steering Group (**JMLSG**), which the FCA takes into account when deciding whether to take enforcement action against a firm.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Regulation 46(1) MLR 2017 requires supervisory bodies to effectively monitor their sectors and take necessary measures to ensure that their members comply with the MLR 2017. Such bodies typically secure compliance through their codes of conduct. Prominent examples include the Solicitors Regulation Authority (**SRA**), which requires law firms to comply with applicable AML legislation in Outcome 7.5 of the SRA Handbook, and the Institute of Chartered Accountants in England and Wales (**ICAEW**) which requires accounting firms to accept client relationships in compliance with AML requirements under paragraphs 210.2 and 210.13 of its code of ethics.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Regulation 49(1)(d) MLR 2017 requires supervisory bodies to ensure that any contravention of the MLR 2017 is met with effective, proportionate and dissuasive disciplinary measures. The Office for Professional Body Anti-Money Laundering Supervision has published guidance which sets out examples of punitive action including public censure, financial penalties and withdrawal of membership. Typically, professional bodies will take steps against members who breach AML requirements. For example, in October 2017, the Solicitors Disciplinary Tribunal struck off a solicitor and ordered payment of GBP 3,337 in costs for laundering of around GBP 100,000 in proceeds from a wine investment scam.

2.4 Are there requirements only at national level?

The MLR 2017 operates at the national level. Equally, the FCA is the regulator for the financial sector across the UK. However, for

the legal and accounting professions, Scotland and Northern Ireland have different supervisory bodies that each have their own code of conduct. It is worth bearing in mind that such codes seek to bring members in compliance with the MLR 2017 and as a result are quite similar. For example, the Institutes of Chartered Accountants of Scotland and Ireland have similar AML provisions in their code of ethics to that of the ICAEW (as described at question 2.2 above).

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

A number of supervisory authorities operating in the UK are required to ensure compliance with and enforcement of anti-money laundering requirements for organisations that fall within the scope of the MLR 2017 (see question 3.1 below).

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The NCA is the UK's designated FIU.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

No statute of limitations applies for criminal offences relating to money laundering (either under POCA or the MLR 2017).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

The maximum penalty for a failure to comply with regulatory/administrative AML requirements is an unlimited fine. Any such fine will be calculated in accordance with the relevant supervisory authority's penalties and enforcement guidance (for example, the FCA's Decision Procedures and Penalties Manual). A significant number of failures to comply with relevant requirements under the MLR 2017 are subject to penalty provisions. These are set out at Schedule 6 to MLR 2017 and include failure to:

(i) carry out risk assessments;
(ii) apply policies and procedures;
(iii) appoint a nominated officer;
(iv) keep required records;
(v) apply customer due diligence measures when required;
(vi) conduct ongoing monitoring of a business relationship; and
(vii) take additional measures in relation to a Politically Exposed Person (**PEP**).

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

In minor cases of non-compliance, a supervisory authority may issue a warning letter to the individual or legal entity.

A company director convicted of a money laundering offence may be disqualified from holding company directorships.

A legal entity may be barred (for a period of time) from tendering for public contracts with EU public bodies if convicted of a money laundering offence.

Self-regulatory organisations also impose sanctions on their professional members (e.g. striking off or withdrawing a licence) for breaches of the MLR 2017. Similarly, by virtue of a breach of the MLR 2017, the FCA or HMRC may find that an individual or entity is no longer a "fit and proper" person and on that basis withhold or withdraw permission or authorisation to carry on certain types of regulated business.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

As indicated in question 2.7 above, in addition to the criminal offences under POCA, the MLR 2017 contain three specific criminal offences relating to violations of AML obligations.

Specifically, Regulation 86 provides that it is a criminal offence to contravene a relevant requirement under the MLR 2017 (set out at Schedule 6 of the MLR 2017 and includes carrying out risk assessments, training and CDD).

Regulation 87 makes it a criminal offence to prejudice a money laundering investigation, either by disclosing that such an investigation is taking place or by falsifying, concealing or destroying any documents relevant to the investigation.

Finally, Regulation 88 makes it a criminal offence to: (a) knowingly or recklessly provide false or misleading information in purported compliance with the MLR 2017; or (b) disclose information in contravention of the MLR 2017.

In each case, the maximum penalty is an unlimited fine or two years' imprisonment.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The specific process for assessment and collection of sanctions and appeal of administrative decisions is dependent on the supervisory authority responsible. In general terms, the imposition by a supervisory authority of a sanction for breaches of the MLR 2017 will be in accordance with their professional disciplinary and conduct rules and published enforcement guidance (for example, the FCA's Decision Procedures and Penalties Manual).

In all cases, there is a right of appeal against a decision imposed by a supervisory authority, for example, to the Administrative Court (for decisions of the Solicitors' Disciplinary Tribunal) or to the Upper Tribunal (for decisions of the FCA).

Absent a compelling reason otherwise (for example, a publication could prejudice an ongoing investigation or cause serious unfairness), hearings relating to and resolutions of penalty actions by supervisory authorities will be public.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The MLR 2017 apply, with a few limited exceptions, to the following entities acting in the course of business in the UK:

- credit institutions *(as defined in Article 4.1(1) of the EU Capital Requirements Regulation (Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms))*;
- financial institutions *(an undertaking, including a money service business, that carries out certain activities (listed in points 2 to 12, 14 and 15 of Annex 1 of the EU Capital Requirements Directive))* including insurance undertakings, investment service providers, bidders in auctions allowed under the emission allowance directive, collective investment undertakings, insurance intermediaries and the National Savings Bank;
- branches of the above;
- auditors, insolvency practitioners, external accountants, tax advisers;
- independent legal professionals;
- trust or company service providers;
- estate agents;
- high value dealers;
- casinos; and
- auction platforms (only some of the MLR 2017 apply).

The MLR 2017 impose requirements concerning risk assessments, ownership and control, AML policies and procedures, internal controls, training, recordkeeping, ongoing monitoring of business relationships, CDD, information on payer and payees (for payment service providers) and ceasing transactions in certain circumstances. Businesses are also compelled to provide information and/or documents to supervising authorities on request.

Additional obligations for financial institutions are contained in the FCA Senior Management Arrangements, Systems and Controls Sourcebook (**SYSC**) which requires regulated financial services firms to have AML systems and controls in place covering additional matters such as governance, documenting risk management policies and considering AML policies when developing new products, taking on new customers and changing business profile. In considering whether a firm has complied with its obligations under the MLR 2017 and SYSC, the FCA will consider whether guidance issued by the JMLSG has been followed – this guidance has been ratified by the UK Treasury.

The UK Criminal Finances Act 2017 imposes further disclosure requirements on financial institutions concerning suspicious transactions and in connection with Unexplained Wealth Orders.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Cryptoassets such as Bitcoin are largely unregulated in the UK. In January 2019, the FCA published a consultation paper with guidance on which types of cryptoassets fall within the existing regulatory regimes. Cryptocurrencies are currently subject to regulation only to the extent that they form part of other regulated services or products, such as cryptocurrency derivatives. In April 2018, the FCA published a statement confirming that cryptocurrency derivatives (including cryptocurrency futures, options and contracts for differences) are capable of being financial instruments under the MiFID II Directive, although they are not considered to be currencies or commodities for regulatory purposes under MiFID II. In the Cryptoasset Taskforce's October 2017 final report, the HM Treasury committed, during 2019, to consult on transposing the Fifth Money Laundering Directive (**5MLD**) as well as wider anti-money laundering and counter terrorist financing requirements to tackle the use of cryptocurrencies for illicit activities. See question 4.1 for more information regarding 5MLD.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes – the MLR 2017 (and, for financial institutions, the SYSC) impose requirements on the businesses listed at question 3.1 above to, where appropriate to the size and nature of its business, have effective AML systems and internal controls in place, including to assess compliance. Required elements include senior responsibility, employee screening, an independent internal audit function to monitor compliance and make recommendations, appointment of a nominated officer responsible for AML compliance, and timely internal reporting.

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There are no specific requirements for recordkeeping or reporting large currency transactions. The general requirements regarding recordkeeping (set out in the MLR 2017 and SYSC as described above) and reporting (set out in POCA and the Terrorism Act 2000 as described above) would, however, apply to such transactions.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No. There are no specific AML requirements for financial institutions or other designated businesses in relation to routinely reporting large non-cash transactions.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

No. There are no specific AML requirements for financial institutions or other designated businesses in relation to cross-border transactions reporting.

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Financial institutions in the UK are required to undertake customer

identification and due diligence work prior to establishing a business relationship with a customer. When entering a new business relationship with a customer, a financial institution must obtain information on:

- the purpose of the business relationship; and
- the intended nature of the relationship (i.e. where funds will come from and the purpose of any contemplated transactions).

The type of information that a financial institution may need to gather from their prospective customer in these circumstances may include:

- details of the customer's business or employment;
- the source and origin of funds that the customer will be using in the business relationship;
- copies of recent and current financial statements;
- details of the relationship between signatories and any underlying beneficial owners; and
- the expected level and type of activity that will take place in the relationship.

This information must be kept updated so that a financial institution can amend its risk assessment of a particular customer if their circumstances change and, if necessary, carry out further due diligence.

In some situations, financial institutions must carry out "enhanced due diligence" prior to establishing a business relationship with a customer. These situations may include:

- when a customer is not physically present when a financial institution carries out its customer identification checks;
- when a financial institution enters into a business relationship with a PEP, which is typically a UK or non-UK domestic member of parliament, head of state or government, or government minister and their family members or known close associates;
- when a financial institution enters into a transaction with a person from a high-risk jurisdiction (as identified by the European Union); and
- any other situation where there may be a higher risk of money laundering.

Enhanced due diligence can include taking some or all of the following steps:

- obtaining further information to establish the customer's identity;
- applying extra measures to check documents supplied by a credit or financial institution; and
- finding out where funds have come from and what the purpose of a particular transaction is.

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Credit and financial institutions (as defined in the MLR 2017) are prohibited from entering into, or continuing, a correspondent relationship with a shell bank (MLR 2017 Reg. 34(2)).

Credit institutions and financial institutions must also take appropriate enhanced measures to ensure that they do not enter into, or continue, a correspondent relationship with a credit institution or financial institution which is known to allow its accounts to be used by a shell bank (MLR 2017 Reg. 34(3)).

The MLR 2017 defines a "shell bank" as a credit institution or financial institution, or an institution engaged in equivalent activities to those carried out by credit institutions or financial institutions, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate or third-country financial conglomerate.

3.9 What is the criteria for reporting suspicious activity?

An obligation to submit a Suspicious Activity Report (**SAR**) to the NCA arises where a firm, its Money Laundering Reporting Officer (**MLRO**) or employees suspect or ought to suspect that anyone (including the firm itself) is or has engaged in money laundering. In broad terms, money laundering is having possession of, or doing anything in relation to, property which the relevant person knows or suspects to represent the benefit of criminal conduct. The threshold for "suspicion" in this context (a possibility which is more than fanciful that the relevant facts exist) is low. The test may be satisfied objectively (i.e. the firm/the individual should suspect) or subjectively (the firm/the individual at the firm does suspect).

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

There is a publicly accessible central government registry (Companies House) for UK company information on management and ownership. However, the ownership information may be up to a year out of date as non-listed companies are only required to provide this information to Companies House annually.

In practice, up-to-date share ownership information regarding shareholdings of 3%+ in a company with shares admitted to trading on a regulated or prescribed market, is publicly available due to stringent notification requirements under the FCA's Disclosure Guidance and Transparency Rules. There is also a public register of Persons with Significant Control (**PCS**s) of companies (over 25% indirect or direct shares or voting rights, significant control or right to appoint or remove majority of directors). Any changes must be notified within 14 days. The register does not, however, extend to UK Crown Dependencies and Overseas Territories. The FAFT report dated 1 December 2018 noted that the register is sometimes inaccurate, and there is no obligation on Companies House to update it at present when notified of inaccuracies.

The Sanctions and Anti-Money Laundering Act 2018 contains provisions on publicly accessible registers of company beneficial ownership in the UK Overseas Territories. Reasonable assistance must be provided to enable each of those governments to establish a publicly accessible register of the beneficial ownership of companies registered in each government's jurisdiction. The Secretary of State must, no later than 31 December 2020, prepare a draft Order in Council requiring the government of any British Overseas Territory that has not introduced a publicly accessible register of the beneficial ownership of companies within its jurisdiction to do so.

In July 2018, the Department for Business, Energy & Industrial Strategy published a draft Registration of Overseas Entities Bill to establish a public register of beneficial ownership for foreign companies owning property in the UK. Its main purpose is to discourage money laundering through greater transparency of property ownership. The Bill includes criminal penalties for non-

compliance as well as restrictions on non-compliant entities wanting to buy or sell property in the UK. The register is expected to become operational in 2021.

The Criminal Finances Act 2017 introduced provisions relating to co-operation and sharing of beneficial ownership information between the UK and "relevant territories", i.e. British Crown Dependencies and Overseas Territories (e.g. the BVI and Cayman Islands). A review of existing arrangements for sharing Overseas Territories' company beneficial ownership information with UK law enforcement authorities was published in May 2018 and found that the systems were working effectively.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Payment Service Providers (**PSP**s) must comply with requirements contained in the MLR 2017, derived from Chapter II, Section 1, Chapter 4 of the EU Funds Transfer Regulation. Complete payer and payee information (name, address, and account number) must generally accompany all wire transfers although there are limited exceptions. For example, if the Payment Service Providers of both payer and payee are located within the EU, then the wire transfer only need be accompanied by at least the account numbers of the payer and payee. Intermediary PSPs must ensure that all information received on the payer and payee which accompanies a wire transfer is retained with the transfer. Guidance provided by the JMLSG provides more detail on how to comply with these requirements and exceptions.

3.12 Is ownership of legal entities in the form of bearer shares permitted?

No. Bearer shares were abolished on 26 May 2015 when amendments to the UK Companies Act 2006 were implemented, via the Small Business, Enterprise and Employment Act 2015.

The changes were made as part of the UK government's aim to promote transparency of company ownership and control to deter criminal misuse of companies in the UK. From 26 May 2015, UK companies were prohibited from issuing bearer shares and companies with bearer shares in issue were required to take action to get rid of them.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Most of the UK money laundering offences described at question 1.2 apply to all businesses, subject to the jurisdictional requirements stated at question 1.3. However, only the businesses listed at question 3.1 (which include certain non-financial institution businesses) can commit the offences of "tipping-off" and "failure to disclose" under POCA. A business not listed at question 3.1 can commit the offence of "failure to disclose" under s332 POCA if it has appointed an MLRO.

The MLR 2017 apply to the businesses listed in question 3.1 above, which includes certain non-financial institution businesses.

There are some specific requirements for payment service providers (**PSP**s). PSPs must comply with additional requirements contained in the MLR 2017, derived from the EU Funds Transfer Regulation. See question 3.11 above.

There are a very small number of sector-specific exceptions to the requirements in the MLR 2017, e.g., Regulation 31 (requirement to cease transactions) does not apply to certain professional advisers advising on the institution or avoidance of legal proceedings, Regulation 32 contains a Customer Due Diligence exception for trustees of debt issues.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Aside from the businesses listed in question 3.1 above, there are no AML requirements applicable to other specific business sectors.

Transaction risk and geographical risk are two of the factors that must be considered as part of a risk assessment of money laundering and terrorist financing, under Regulation 18(2)(b) MLR 2017, by the businesses listed in question 3.1 above.

Guidance from JMLSG provides some sectoral guidance for the UK financial sector, on managing money laundering risk in certain business areas (e.g. trade finance, correspondent banking, wealth management). Whilst the guidance is not binding, it would be taken into account by enforcement authorities when deciding whether or not a firm, or an individual, has complied with their AML requirements under POCA 2002 or the MLR 2017. Some supervisory bodies have also produced guidance for members (e.g. the UK Law Society).

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

On Brexit, the MLR 2017 will be amended by the Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019 (2019 No. 253), just to the extent necessary to reflect the fact that the UK will no longer be an EU Member State. The main changes would be:

- Equalisation of due diligence requirements applied to intra-EEA correspondent banking relationships (to bring in line with non-EEA banks).
- European Commission's high-risk third country list will be "on shored" (i.e. become part of UK law as at a particular date) but will not be dynamic – i.e. will not track changes at EU level – the list will only evolve as amended by UK law.
- New powers for the FCA to make technical standards to specify what additional measures are required to be taken by credit and financial institutions with branches or subsidiaries abroad. This function is currently exercised by the European Commission.
- Equalisation of information requirements for fund transfers both in and outside the EU. The effect of this will be to require UK PSPs to provide greater volumes of information accompanying transfers of funds into EU Member States than is currently the case.
- Removal of mandatory regard to guidelines published by the European Supervisory Authorities (although they are still likely to be taken into account by the FCA).
- Removal of need for transmission of information (such as the UK's National Risk Assessments of Money Laundering and Terrorist Financing) to EU institutions and other Member States.

The UK Government has stated that it will implement **5MLD**. Provisions relating to anonymous safe deposit boxes have already come into force. The rest is due to be transposed by 10 January 2020.

5MLD expands the requirement to perform anti-money laundering checks to new categories of businesses (e.g. custodian wallet providers and virtual currency exchange platforms) and increases transparency requirements for the beneficial ownership of both companies and trusts. The UK declined to opt-in to the Sixth AML Directive (**6MLD**). When declining to opt-in, the UK government reported to Parliament that the UK is already "largely compliant" with 6MLD's measures in any event.

The Sanctions and Anti-Money Laundering Act 2018 creates a new UK legislative framework with broad powers to implement sanctions, anti-money laundering and anti-terrorist financing measures if the UK leaves the European Union.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

The Report on the Fourth Round Mutual Evaluation of the UK by the FAFT dated 1 December 2018 concluded that "the UK's overall AML/CFT regime is effective in many respects. It needs to address certain areas of weakness, such as supervision and the reporting and investigation of suspicious transactions. However, the country has demonstrated a robust level of understanding of its risks, a range of proactive measures and initiatives to counter the significant risks identified and plays a leading role in promoting global effective implementation of AML/CFT measures".

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The Report on the Fourth Round Mutual Evaluation of the UK by the FAFT was published on 1 December 2018. The IMF conducted a Financial Sector Assessment Programme (**FSAP**) for the UK in the areas of AML/CFT in 2016.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The FCA provides comprehensive information on the applicable laws and guidelines in money laundering and terrorist financing. (www.fca.org.uk).

The UK Parliament website contains the relevant Bills of Parliament, secondary legislation and information on parliament debates, committee reports and proposed new laws (www.parliament.uk).

Mona Vaswani
Allen & Overy LLP
Bishops Square
London, E1 6AD
United Kingdom

Tel: +44 20 3088 3751
Email: mona.vaswani@allenovery.com
URL: www.allenovery.com

Mona Vaswani is co-head of the firm's UK Banking, Finance and Regulatory Litigation practice and head of the Fraud Practice.

Mona advises on a variety of complex, cross-border disputes with an emphasis on banking litigation, fraud and asset tracing claims as well as trust litigation. She has substantial experience in advising banks and trustees, in particular offshore trustees in the conduct of trust litigation in several jurisdictions. Mona has acted in various claims in the High Court including those involving allegations of fraud, constructive trust and breach of fiduciary duty.

Amy Edwards
Allen & Overy LLP
Bishops Square
London, E1 6AD
United Kingdom

Tel: +44 20 3088 2243
Email: amy.edwards@allenovery.com
URL: www.allenovery.com

Amy Edwards is a Senior Professional Support Lawyer in the London Litigation practice with particular expertise in commercial law and financial crime. With over 20 years' experience, Amy has advised widely on dispute resolution relating to financial institutions, corporations and individuals in domestic and international criminal and civil matters.

ALLEN & OVERY

Allen & Overy LLP's market-leading global investigations practice advises clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The global team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in the U.S. and Europe. We have offices in 31 jurisdictions and offer global expertise in handling investigations, and associated employee issues. We have leading criminal defence capability covering anti-corruption and bribery, anti-money laundering, fraud (financial and tax), antitrust, sanctions and insider dealing. As a result, we are able to assist clients to minimise the risks of navigating the complex, and often conflicting, issues that arise when handling information in cross-border investigations.

Chapter 35

USA

Joel M. Cohen

Linda Noonan

Gibson, Dunn & Crutcher LLP

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at national level?

Money laundering has been a crime in the United States since 1986, making the United States one of the first countries to criminalise money laundering conduct. There are two money laundering criminal provisions, 18 United States Code, sections 1956 and 1957 (18 U.S.C. §§ 1956 and 1957).

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Generally, it is a crime to engage in virtually any type of financial transaction if a person conducted the transaction with knowledge that the funds were the proceeds of "criminal activity" and if the government can prove the proceeds were derived from a "specified unlawful activity". Criminal activity can be a violation of any criminal law – federal, state, local, or foreign. Specified unlawful activities are set forth in the statute and include over 200 types of U.S. crimes, from drug trafficking, terrorism, and fraud, to crimes traditionally associated with organised crime, and certain foreign crimes, as discussed below in question 1.3.

The government does not need to prove that the person conducting the money laundering transaction knew that the proceeds were from a specified form of illegal activity.

Knowledge can be based on wilful blindness or conscious indifference – failure to inquire when faced with red flags for illegal activity. Additionally, knowledge can be based on a government "sting" or subterfuge where government agents represent that funds are the proceeds of illegal activity.

Under Section 1956, the transaction can be: (1) with the intent to promote the carrying on of the specified unlawful activity; (2) with the intent to engage in U.S. tax evasion or to file a false tax return; (3) knowing the transaction is in whole or in part to disguise the nature, location, source, ownership or control of the proceeds of a specified unlawful activity; or (4) with the intent to avoid a transaction reporting requirement under federal or state law.

Section 1956 also criminalises the transportation or transmission of funds or monetary instruments (cash or negotiable instruments or securities in bearer form): (1) with the intent to promote the carrying out of a specific unlawful activity; or (2) knowing the funds or monetary instruments represent the proceeds of a specified unlawful activity and the transmission or transportation is designed in whole or in part to conceal or disguise the nature, location, source, ownership or control of the proceeds of the specified unlawful activity.

Under Section 1957, it is a crime to knowingly engage in a financial transaction in property derived from specified unlawful activity through a U.S. bank or other "financial institution" or a foreign bank (in an amount greater than $10,000). Financial institution is broadly defined with reference to the Bank Secrecy Act ("BSA") statutory definition of financial institution (31 U.S.C. § 5312(a)(2)) and includes not just banks, but a wide range of other financial businesses, including securities broker-dealers, insurance companies, non-bank finance companies, and casinos.

Tax evasion is not itself a predicate offence, but, as noted, conducting a transaction with the proceeds of another specified unlawful activity with the intent to evade federal tax or file a false tax return is subject to prosecution under Section 1956. Also, wire fraud (18 U.S.C. § 1343) is a specified unlawful activity. Wire fraud to promote tax evasion, even foreign tax evasion, can be a money laundering predicate offence. *See U.S. v. Pasquantino*, 544 U.S. 349 (2005) (wire fraud to defraud a foreign government of tax revenue can be a basis for money laundering).

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

There is extensive extraterritorial jurisdiction under the money laundering criminal provisions. Under Section 1956, there is extraterritorial jurisdiction over money laundering conduct (over $10,000) by a U.S. citizen anywhere in the world or over a non-U.S. citizen if the conduct occurs at least "in part" in the United States. "In part" can be a funds transfer to a U.S. bank.

Under Section 1957, there is jurisdiction over offences that take place outside the United States by U.S. persons (citizens, residents, and legal persons) and by non-U.S. persons as long as the transaction occurs in whole or in part in the United States.

Certain foreign crimes are specified unlawful activities, including drug crimes, murder for hire, arson, foreign public corruption, foreign bank fraud, arms smuggling, human trafficking, and any crime subject to a multilateral extradition treaty with the United States.

Generally, there is no extraterritorial jurisdiction under the BSA, discussed below in section 2. The BSA requirements for Money Services Businesses ("MSBs") can apply, however, even if the MSB

has no physical presence in the United States if the business conducts business "wholly or in substantial part within the United States", *i.e.*, if a substantial number of U.S. customers or recipients of funds transfers are in the United States. 31 C.F.R. § 1010.100(*ff*) (BSA definition of MSB).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Prosecution of money laundering crimes is the responsibility of the U.S. Department of Justice. There is a special unit in the Criminal Division of the Department of Justice, the Money Laundering and Asset Recovery Section ("MLARS"), that is responsible for money laundering prosecution and related forfeiture actions. The 94 U.S. Attorney's Offices across the United States and its territories also may prosecute the crime of money laundering alone or with MLARS. MLARS must approve any prosecution of a financial institution by a U.S. Attorney's Office.

As required in Section 1956(e), there is a (non-public) memorandum of understanding among the Secretary of the Treasury, the Secretary of Homeland Security, the Attorney General, and the Postal Service setting forth investigative responsibilities of the various federal law enforcement agencies that have investigative jurisdiction over Sections 1956 and 1957. Jurisdiction is generally along the lines of the responsibility for the underlying specified unlawful activity. The various federal agencies frequently work together on cases, sometimes along with state and local authorities, where jurisdiction overlaps.

The Federal Bureau of Investigation, the Drug Enforcement Administration, the U.S. Secret Service, U.S. Immigration and Customs Enforcement, the Internal Revenue Service Criminal Division, and the Postal Inspection Service frequently conduct money laundering investigations. An investigation unit of the Environmental Protection Agency can investigate money laundering crimes relating to environmental crimes.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is criminal liability for natural and legal persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalties are fines up to $500,000 or double the amount of property involved, whichever is greater, for each violation, and for individuals, imprisonment up to 20 years for each violation.

1.7 What is the statute of limitations for money laundering crimes?

That statute of limitations is five years. 18 U.S.C. § 3282(a).

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Section 1956(d) specifically provides that it does not supersede any provisions in federal, state or other local laws imposing additional criminal or civil (administrative) penalties.

Many states, including New York and California, have parallel money laundering criminal provisions under state law. *See, e.g.*, New York Penal Law Article 470.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

There is both criminal forfeiture following a conviction for money laundering, and civil forfeiture against the assets involved in, or traceable to, money laundering criminal conduct.

Under 18 U.S.C. § 982, if a person has been convicted of money laundering, any property, real or personal, involved in the offence, or any property traceable to the offence, is subject to forfeiture.

Under 18 U.S.C. § 981, a civil forfeiture action can be brought against property involved in or is traceable to the money laundering conduct even if no one has been convicted of money laundering. Because this is a civil action, the standard of proof for the government is lower than if there were a criminal prosecution for the money laundering conduct (preponderance of the evidence versus beyond a reasonable doubt). There is no need to establish that the person alleged to have committed money laundering is dead or otherwise unavailable.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Absent established collusion with money launderers or other criminals, very few directors, officers, or employees have been convicted of money laundering. Where there have been criminal settlements with banks and other financial institutions related to money laundering, in all but one case, the settlements have been based on alleged violations of the Bank Secrecy Act ("BSA"), not violations of the money laundering criminal offenses.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Since 2002, 34 regulated financial institutions (25 banks) have pled guilty or have reached criminal settlements with the Department of Justice, generally, as noted, based on alleged violations of the anti-money laundering regulatory requirements under the BSA (either failure to maintain an adequate anti-money laundering program and/or failure to file required Suspicious Activity Reports). In one of these cases, a casino entered a settlement based on alleged violations of the money laundering criminal offenses.

A few of these settlements with foreign-owned banks have been based on alleged sanctions violations in addition to BSA violations. Substantial fines or forfeitures were paid as part of these settlements. There also were two other BSA prosecutions of banks in the late 1980s relating to currency transaction reporting and Bank of Credit and Commerce International ("BCCI") pled guilty to money laundering in 1990.

In connection with many of the criminal dispositions, civil (administrative) sanctions based on the same or related misconduct have been imposed at the same time by federal and/or state regulators and the Financial Crimes Enforcement Network ("FinCEN") in a coordinated settlement. *See* questions 2.8–2.11.

One reason criminal settlements with banks may not be based on the money laundering statute may be the severe potential legal

consequences or "death penalty" for a bank if it is convicted of money laundering. If a bank is convicted of money laundering, subject to a required regulatory (administrative) hearing, the bank could lose its federal deposit insurance, *i.e.*, be forced to cease operations. Such a review is discretionary if a bank is convicted of BSA violations and, in practice, not conducted. *See, e.g.*, 12 U.S.C. § 1818(w) (process for state-licensed, federally-insured banks).

Records relating to the criminal settlements are publicly available, including, in most cases, lengthy statements by the government about underlying facts that led to the criminal disposition. To our knowledge, there have been no non-public criminal settlements with financial institutions.

2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Authorities

In the United States, the main anti-money laundering ("AML") legal authority is the Bank Secrecy Act, 31 U.S.C. § 5311 *et seq.*, 12 U.S.C. §§ 1829b and 1951–1959 (the "BSA statute"), and the Bank Secrecy Act implementing regulations, 31 C.F.R. Chapter X (the "BSA regulations"). (The BSA statute and regulations collectively will be referred to as "the BSA".) The BSA statute was originally enacted in 1970 and has been amended several times, including significantly in 2001 by the USA PATRIOT Act ("PATRIOT Act"). The BSA gives the Secretary of the Treasury the authority to implement reporting, recordkeeping, and anti-money laundering program requirements by regulation for financial institutions and other businesses listed in the statute. 31 U.S.C. § 5312(a)(2). The Secretary of the Treasury has delegated the authority to administer and enforce the BSA to a Department of the Treasury bureau, FinCEN. FinCEN also is the U.S. Financial Intelligence Unit. *See* question 2.6. Because FinCEN has no examination staff, it has further delegated BSA examination authority for various categories of financial institutions to their federal functional regulators (federal bank, securities, and futures regulators). Examination authorities for financial institutions and businesses without a federal functional regulator is discussed in question 2.5.

The federal banking regulators (the Office of the Comptroller of the Currency (the "OCC"), the Board of Governors of the Federal Reserve ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA")) have parallel regulatory authority to require BSA compliance programs and suspicious activity reporting for the institutions for which they are responsible. *See, e.g.*, 12 C.F.R. §§ 21.21 (OCC BSA program requirement), 21.12 (OCC suspicious activity reporting requirement). Consequently, the bank regulators have both delegated examination authority from FinCEN, as federal functional regulators, and independent regulatory enforcement authority.

BSA examination authority for broker-dealers has been delegated to the Securities and Exchange Commission ("SEC"), as the federal functional regulator for broker-dealers. The SEC has further delegated authority to the Financial Industry Regulatory Authority ("FINRA"), the self-regulatory organization ("SRO") for broker-dealers. The SEC also has incorporated compliance with the BSA requirements for broker-dealers into SEC regulations and, consequently, has independent authority to enforce the BSA. 17 C.F.R. §§ 240.17a-8, 405.4.

Similarly, BSA examination authority for futures commission merchants ("FCMs") and introducing brokers in commodities ("IB-Cs"), which are financial institutions under the BSA, has been delegated by FinCEN to the Commodities Futures Trading Commission ("CFTC"), as their federal functional regulator. The CFTC also has incorporated BSA compliance in its regulations. 17 C.F.R. § 42.2. The CFTC has delegated authority to the National Futures Authority ("NFA") as that industry's SRO.

AML Requirements

For the United States, the response to the question of what requirements apply is complicated. The BSA statute generally is not self-executing and must be implemented by regulation. The scope and details of regulatory requirements for each category of financial institutions and financial businesses subject to BSA vary. To further complicate the issue, all these businesses are defined as financial institutions under the BSA statute, but only certain ones are designated as financial institutions under the BSA regulations, *i.e.*, banks, broker-dealers, FCMs, IB-Cs, mutual funds, MSBs, casinos, and card clubs. Some BSA requirements only apply to businesses that come within the BSA definition of financial institution.

There also are three BSA requirements that apply to all persons subject to U.S. jurisdiction or to all U.S. trades businesses, not just to financial institutions or other businesses subject to specific BSA regulatory requirements. *See* question 3.13.

Main Requirements

These are the main requirements that apply under the BSA regulations, most of which are discussed in more detail in Part 3, as cross-referenced below.

AML Programs: All financial institutions and financial businesses subject to the BSA regulations are required to maintain risk-based AML Programs with certain minimum requirements to guard against money laundering. *See* questions 3.1, 3.2 and 3.3.

Currency Transaction Reporting: "Financial institutions" as defined under the BSA regulations must file Currency Transaction Reports ("CTRs"). *See* question 3.4.

Cash Reporting or Form 8300 Reporting: This requirement applies to all other businesses that are subject to the AML Program requirement, but not defined as financial institutions under the BSA regulations, and all other U.S. trades and businesses. *See* questions 3.4 and 3.13.

Suspicious Transaction Reporting: Financial institutions and other businesses subject to the AML Program requirement (except Check Cashers, Operators of Credit Card Systems, and Dealers in Precious Metals, Precious Stones, or Jewels) must file Suspicious Activity Reports ("SARs"). *See* question 3.9.

Customer Due Diligence (CDD) Programs: Banks, broker-dealers, FCMs, IB-Cs, and mutual funds are required to maintain CDD programs. *See* question 3.7.

Customer Identification Program ("CIP"): Certain BSA financial institutions (banks, broker-dealers, FCMs, IB-Cs, and mutual funds) are required to maintain CIP programs as part of their CDD and AML Programs. *See* question 3.7.

Customer Due Diligence Programs for Non-U.S. Private Banking Clients and Foreign Correspondents: This requirement is applicable to banks, broker-dealers, FCMs, IB-Cs, and mutual funds. *See* question 3.7.

Recordkeeping: There are BSA general recordkeeping requirements applicable to all BSA financial institutions, specific recordkeeping

requirements for specific types of BSA financial institutions, and requirements to maintain records related to BSA compliance for all financial institutions and financial businesses subject to the BSA. Generally, records are required to be maintained for five years. 31 C.F.R. § 1010.400 (general recordkeeping requirements for financial institutions); *see, e.g.*, 31 C.F.R. § 1023.410 (recordkeeping requirements for broker-dealers).

Cash Sale of Monetary Instruments: There are special recordkeeping and identification requirements relating to the cash sale of monetary instruments in amounts of $3,000 to $10,000 inclusive (bank checks or drafts, cashier's checks, travellers' cheques, and money orders) by banks and other financial institutions under the BSA regulations. 31 C.F.R. § 1010.415.

Funds Transfer Recordkeeping and the Travel Rule: This is applicable to banks and other financial institutions under the BSA regulations. *See* question 3.11.

Money Services Business Registration: MSBs must register (and re-register every two years) with FinCEN. MSBs that are only MSBs because they are agents of another MSB are not required to register. MSBs must maintain lists of their agents with certain information and provide the lists to FinCEN upon request. Sellers of prepaid access (unless MSBs by virtue of other business activities) are excepted from registration. 31 C.F.R. § 1022.380.

Government Information Sharing or Section 314(a) Sharing: Periodically and on an *ad hoc* basis, banks, broker-dealers, and certain large MSBs receive lists from FinCEN of persons suspected of terrorist activity or money laundering by law enforcement agencies. The financial institutions must respond with information about accounts maintained for the persons and certain transactions conducted by them in accordance with guidance from FinCEN that is not public. The request and response are sent and received via a secure network. Strict confidentiality is required about the process. 31 C.F.R. § 1010.520.

Voluntary Financial Institution Information Sharing or Section 314(b) Sharing: Financial institutions or other businesses required to maintain AML Programs under the BSA regulations may voluntarily register with FinCEN to participate in sharing information with each other. The request can only be made for the purpose of identifying and/or reporting activity that the requestor suspects may be involved in terrorist activity or money laundering. The information received may only be used for SAR filing, to determine whether to open or maintain an account or conduct a transaction, or for use in BSA compliance. Strict confidentiality about the process must be maintained by participants. If all requirements are satisfied, there is a safe harbour from civil liability based on the disclosure. 31 C.F.R. § 1010.540.

Section 311 Special Measures: Under Section 311 of the PATRIOT Act, FinCEN can impose a range of special measures against a foreign jurisdiction or foreign financial institution that is designated as posing primary money laundering concern. One of the measures frequently imposed is to prohibit U.S.-covered financial institutions (banks, broker-dealers, FCMs, IB-Cs, and mutual funds) from providing correspondent accounts directly or indirectly to the financial institutions subject to special measures and to notify their correspondent accountholders that they cannot offer services to the designated financial institutions through their correspondent account with the U.S. institution.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

As discussed in question 2.1, the SROs for the securities and futures industries have imposed requirements on their members and share examination and enforcement authority with the federal functional regulators, the SEC and CFTC, respectively.

With the approval of the SEC, FINRA has issued AML Program requirements for broker-dealers, under FINRA Rule 3310, and the NFA has issued AML Program requirements, under NFA Compliance Rule 2-9(c) for FCMs and IB-Cs. *See* question 2.1.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

FINRA examines broker-dealers for compliance with AML Program requirements and, more frequently than any regulatory agency, brings enforcement actions against its members, which can include civil penalties against firms and individual officers and employees (including AML compliance officers), compliance undertakings, and in some cases, termination of firms and suspension or revocation of licences of officers and employees. The NFA also has brought similar enforcement actions based on examinations of FCMs and IB-Cs.

2.4 Are there requirements only at national level?

Many states impose parallel requirements on state-licensed financial institutions, *e.g.*, state-licensed banks and money services businesses, such as check cashers and money transmitters. Coverage and requirements vary by state.

The New York Department of Financial Services ("DFS") is the most active state regulator in AML and sanctions enforcement. In some recent cases, it has brought enforcement actions with large civil monetary penalties against New York branches and subsidiaries of foreign banks even where no federal regulator has imposed a penalty. The actions are based on the banks' failures to maintain books and records under New York law relating to their alleged BSA and sanctions failures. New York Banking Law §§ 39 (books and records provision), 44 (penalty provisions). In connection with one enforcement action, DFS also required a foreign bank to surrender the license of its branch to do business in New York.

New York also requires suspicious activity reporting by New York-licensed financial institutions, which has been interpreted to include reporting of potential money laundering activity. 3 N.Y.C.R.R. Part 300.

New York has implemented a unique requirement in Part 504 of the Banking Superintendent's Regulations, which is applicable to New York-licensed banks, check cashers, and money transmitters. Part 504 requires annual compliance statements, *i.e.*, certifications, by a resolution of the Board of Directors or a "compliance finding" by a senior officer confirming that: (1) the financial institution maintains a risk-based transaction monitoring system to identify potential suspicious activity for purposes of compliance with the BSA suspicious activity reporting requirement (and a risk-based sanctions filtering system to comply with sanctions requirements); and (2) certain facts relating to the maintenance, design, and implementation of those systems. The first annual board resolution or senior officer compliance finding under Rule 504 was due on April 15, 2018. NYDFS Superintendent's Regulations § 504.1-6. There are concerns about the potential liability for those making the certifications or confirming statements if subsequent compliance issues are identified.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Responsible Authorities

As discussed in question 2.1, FinCEN does not have examination staff and has delegated an examination authority to the federal functional regulators for the financial institutions for which they are responsible. The federal functional regulators are: the OCC; Federal Reserve; FDIC; NCUA; SEC (broker-dealers and mutual funds); and CFTC (FCMs and IB-Cs). The SEC and CFTC retain authority, but also have delegated authority to the SROs, FINRA and NFA.

Examination responsibility for the housing government-sponsored enterprises (the Federal Home Loan Mortgage Corporation ("Freddie Mac") and the Federal National Mortgage Association ("Fannie Mae")) is with the Federal Housing Finance Agency, the conservator for these entities.

For all other financial institutions and businesses subject to AML Program requirements, the examination authority has been delegated to the Internal Revenue Service ("IRS"). This includes money services businesses, casinos, card clubs, insurance companies (with respect to certain products), dealers in precious metals, precious stones, and jewels, operators of credit card systems and non-bank residential mortgage originators and lenders.

FinCEN has entered a number of agreements with state insurance commissioners providing for BSA examinations of insurance companies by state insurance examiners.

Examination Criteria

The most useful public guidance is the *Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual* for banks ("FFIEC Manual"), available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

This manual was originally compiled by FinCEN and other federal banking agencies in 2006 and, with the exception of two chapters (the CDD chapter and a new chapter on beneficial ownership) updated in 2018, was last updated in 2014. The next comprehensive update is expected in 2019.

FinCEN and the IRS published a *Bank Secrecy Act/Anti-Money Laundering Examination Manual* for Money Services Businesses in 2008, which has not been updated, available at https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf.

There are no analogous published examination criteria for the other sectors subject to the BSA.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

FinCEN is the U.S. FIU responsible for analysing and disseminating information reported under the BSA in addition to interpreting the BSA, promulgating BSA regulatory requirements, and exercising civil (administrative) BSA enforcement authority.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

The federal functional regulators have a five-year statute of limitations for BSA-related enforcement actions. There is a six-year statute of limitations for civil actions, and there is a five-year statute of limitations for criminal violations of the BSA. 31 U.S.C. § 5321(b) (civil) and 18 U.S.C § 3282(a) (criminal).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

BSA civil and/or criminal penalties may be imposed against financial institutions and other businesses subject to the BSA and/or their officers, directors, and employees. The penalties vary for different types of violations. Both civil and criminal penalties can be imposed on the same violation, or just civil penalties, or, in a few cases, just criminal penalties. 31 U.S.C. § 5321; 31 C.F.R. § 1010.820. *See* question 2.10.

For instance, if there is a willful failure to report a transaction, the maximum BSA civil penalty is generally $25,000 or the amount of funds involved in the transaction, not to exceed $100,000, whichever is greater, for each transaction involved. 31 C.F.R. § 1010.820.

BSA violations of the AML Program requirement are punished separately for each day the violation continues.

The federal functional regulators and SROs have separate civil money penalty authorities. For instance, the federal banking regulators have a general civil money penalty authority that applies to all violations of laws or regulations, including BSA violations. The maximum penalty depends on the financial institution or employee's intent. Maximum penalties range from $5,000 per violation to $1,000,000, or 1% of the assets of the institution, whichever is greater, per day that the violation continues. 12 U.S.C. § 1818(i).

Penalties generally are assessed for deficiencies in one or more of the required elements of the AML Program requirements, for failure to file Suspicious Activity Reports, or in combination with other BSA violations.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

FinCEN or the federal functional regulators may impose a wide range of undertakings in addition to imposing civil money penalties depending on the alleged deficiencies. For instance, a financial institution could be required to hire a competent BSA/AML Officer, hire qualified independent third parties acceptable to the regulators to perform certain functions, conduct "look-backs" to review transactions to identify previously unreported suspicious activity, or conduct Know Your Customer "look-backs" to upgrade customer files.

In the most egregious cases, individuals can be suspended, restricted, or barred from future employment in the sector, or in the case of FinCEN, from employment at any BSA financial institution.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

As noted, both criminal and civil money penalties can be imposed for the same violation. In general, the maximum BSA criminal penalty is $250,000 and five years' imprisonment for individuals for each violation, or if part of a pattern involving more than $100,000 in a 12-month period while violating another U.S. criminal law, $500,000 and 10 years' imprisonment for individuals. 31 U.S.C. § 5322.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

The process varies depending on the regulator or SRO. There are formal administrative appeals processes by all competent authorities except FinCEN. While FinCEN provides an opportunity to be heard when an enforcement action is proposed, the process is informal and not required by law or regulation.

All actions that include civil money penalties are public. Bank regulators may take "informal" enforcement actions for less serious deficiencies without imposing monetary penalties, which are not public. In theory, if a party failed to comply with the terms of an enforcement action or refused to pay a civil money penalty, there could be a judicial action, but that does not happen in practice because financial institutions have generally not challenged assessments.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

The following are subject to the requirement to maintain risk-based AML Programs:

- Banks, including savings associations, trust companies, credit unions, branches and subsidiaries of foreign banks in the United States, and Edge corporations.
- Broker-dealers in securities.
- Mutual funds.
- Futures Commission Merchants and Introducing Brokers in Commodities.
- Money Services Businesses.
  i. Dealers in foreign exchange.
  ii. Cheque cashers.
  iii. Money transmitters
  iv. Issuers and sellers of travellers' cheques and money orders.
  v. Providers and sellers of prepaid access.
- Insurance companies (only with respect to life insurance and insurance products with investment features).
- Casinos and Card Clubs.
- Operators of Credit Card Systems.
- Non-bank Mortgage Lenders and Originators.
- Dealers in Precious Metals, Precious Stones, or Jewels.
- Housing Government-Sponsored Enterprises.

As discussed in question 2.1, all of the above are subject to either CTR reporting or Form 8300 cash reporting. All but Cheque Cashers, Dealers in Precious Metals, Precious Stones, or Jewels, and Operators of Credit Card Systems are required to file SARs. All have recordkeeping requirements and can participate in Section 314(b) information sharing.

As discussed in question 2.1, certain requirements only apply to banks, broker-dealers, FCM, IB-Cs, and mutual funds:

- CIP.
- Section 312 due diligence programs for private banking accounts for non-U.S. persons and foreign correspondent accounts.
- Prohibition on shell banks.
- New CDD Program requirements.

Certain requirements only apply to those within the BSA definition of financial institution, i.e., banks, broker-dealers, FCMs, IB-Cs, mutual funds, MSBs, casinos, and card clubs:

- CTR reporting.
- Funds transfer recordkeeping and the Travel Rule.
- Recordkeeping for cash sales of monetary instruments.

Companies that offer new payment technologies or alternative currencies may be subject to BSA requirements as MSBs, including the requirement to register with FinCEN, if their activities come under the definition of MSB as a money transmitter or provider of prepaid access. These companies can apply to FinCEN for an administrative ruling to determine their status under the BSA if it is not clear under the regulations. As discussed in question 3.2, FinCEN considers administrators and exchangers of virtual currency to be MSBs.

Currently, investment funds other than mutual funds are not subject to AML requirements. There are pending BSA regulations that will require SEC-registered investment advisers to maintain AML Programmes and file Suspicious Activity Reports. Most investment funds will then be subject to AML requirements indirectly because of the obligations of their investment advisers. Proposed Requirements for Investment Advisers, 80 Federal Register 52680 (Sept. 1, 2015).

Non-bank finance companies, other than residential mortgage lenders and originators, and pawnbrokers are not subject to BSA regulatory requirements although the BSA statute provides authority to apply BSA requirements to them.

Gatekeepers – lawyers, accountants, company formation agents – are not subject to any BSA requirements.

Title insurance companies and other persons involved in real estate closings and settlements are not subject to routine BSA requirements, although the BSA statute provides authority to apply BSA requirements to them. However, as discussed in question 3.13 below, on a temporary basis, title insurance companies in seven U.S. metropolitan areas have been subject to certain reporting requirements. FinCEN also encourages real estate agents, escrow agents, title companies, and others involved in real estate transactions to file SARs voluntarily.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

In 2013, FinCEN issued guidance that administrators and exchangers of virtual currency are money transmitters under the BSA and consequently, are subject to the BSA MSB requirements for AML programs, suspicious activity reporting, and FinCEN registration. FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/sites/default/ files/shared/FIN-2013-G001.pdf.

3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All the financial institutions and financial businesses subject to the BSA (listed in question 3.1) are required to maintain risk-based AML Programs to guard against money laundering with four minimum requirements, sometimes referred to as the four pillars of a program: (1) policies, procedures and internal controls; (2) designation of a compliance officer; (3) training; and (4) periodic independent testing of the program. For financial institutions subject to the CIP requirements (banks, broker-dealers, FCMs and IB-Cs, and mutual funds), the financial institution's CIP must be part of the AML Program. Similarly, for these same financial institutions, new CDD Program requirements and due diligence programs under Section 312 must be part of their AML Programs.

There is a regulatory expectation that the program be executed in accordance with a formal risk assessment. As noted, the authority for specific program requirements may be found in the BSA regulations, the regulations of the federal functional regulator or a rule of the SRO. 31 U.S.C. § 5318(h) (statutory requirement for AML Programs); *see, e.g.*, 31 C.F.R. § 1022.210 (AML Program requirements for MSBs).

3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Currency Transaction Reporting:

Financial institutions (defined as financial institutions under the BSA regulations) must file CTRs with FinCEN on all transactions in (physical) currency in excess of $10,000 (or the foreign equivalent) conducted by, through, or to the financial institution, by or on behalf of the same person, on the same day. 31 C.F.R. § 1010.310–315.

It is prohibited to "structure" transactions to cause a financial institution not to file a CTR or to file an inaccurate CTR by breaking down transactions into smaller amounts at one or more financial institutions over one or more days. 31 C.F.R. § 1010.314.

Banks (and only banks) may exempt the transactions of certain customers from CTR reporting if BSA requirements relating to exemptions are followed. 31 C.F.R. § 1020.315.

Cash Reporting or Form 8300 Reporting:

Other businesses subject to the AML Program requirements, but not defined as financial institutions under the BSA regulations, are subject to the requirement to report on cash *received* in excess of $10,000 (or the foreign equivalent) by the same person on the same day or in one or a series of related transactions on one or more days. Under some circumstances, cash can include cash-equivalent monetary instruments (bank cheques or drafts, cashier's cheques, money orders, and travellers' cheques) for reporting purposes. Insurance companies, operators of credit card systems, dealers in precious metals, precious stones, or jewels, non-bank mortgage lenders and originators, and housing government-sponsored enterprises are subject to Form 8300 reporting, and not to CTR reporting, to the extent they receive currency.

Under the BSA and parallel requirements under the Internal Revenue Code, the same cash reporting requirements apply to all trades or businesses in the United States without respect to whether other BSA requirements apply to them. 31 C.F.R. § 1010.330.

3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, with the exception of requirements imposed on a temporary basis under BSA Geographic Targeting Orders. *See* question 3.14.

3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

With some exceptions for financial institutions, all persons who transport, mail, or ship (or cause to be transported, mailed, or shipped) currency and/or other "monetary instruments" into or out of the United States in the amount of $10,000 or more (or the foreign equivalent) must file a Currency and Other Monetary Instrument Report ("CMIR") with U.S. Customs and Border Protection.

Monetary instruments in this context include travellers' cheques in any form, checks signed with the payee name blank, negotiable instruments, and securities in bearer form, in addition to currency. 31 C.F.R. §§ 1010.340 (CMIR requirement), 1010.100(dd) (definition of monetary instrument).

3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Customer Due Diligence:

Pursuant to regulatory requirements, which became effective May 11, 2018, as part of their AML Programmes, certain financial institutions (banks, broker-dealers, mutual funds, FCMs and IB-Cs) must implement formal risk-based CDD programs that include certain minimum elements, including customer identification and verification (under a Customer Identification Program), obtaining information about the nature and purpose of a customer's account, ongoing monitoring of customer accounts, obtaining beneficial ownership information at a 25% threshold for legal entity customers and identifying a control person for legal entity customers (with certain exceptions). *See, e.g.*, 31 C.F.R. § 1020.210 (AML Program requirements for banks); 31 C.F.R. § 1010.230 (beneficial ownership requirements).

There also is a specific BSA requirement to maintain CDD programs for non-U.S. persons' private banking accounts and foreign correspondent accounts. The same covered financial institutions as for CDD programs (banks, broker-dealers, mutual funds, FCMs and IB-Cs) must maintain a CDD program for non-U.S. private banking accounts established on behalf of, or for the benefit of, a non-U.S. person and foreign correspondent customers and an enhanced due diligence ("EDD") program for those relationships posing a higher risk. These programs must be designed to detect and report suspicious activity with certain minimum standards. These requirements are based on Section 312 of the PATRIOT Act and are often referred to as Section 312 requirements. 31 C.F.R. §§ 1010.610 (due diligence for foreign correspondent accounts), 1010.620 (due diligence for private banking for non-U.S. persons).

Even before the new CDD requirements, for many years, FinCEN and the federal functional regulators expected risk-based CDD to be a core component of AML Programs, with EDD expected for higher risk customers. The FFIEC Manual is a useful reference for which customers should be considered higher risk, *e.g.*, MSBs, non-government organisations, and Politically-Exposed Persons ("PEPs").

Customer Identification Program:

The same financial institutions subject to the CDD requirements, (banks, broker-dealers, mutual funds, and FCMs and IB-Cs) are required to maintain CIPs setting forth how they will comply with the CIP regulatory requirements. The CIP regulations require financial institutions to obtain and record basic identification information (name, street address, date of birth, and identification number for an individual), and verify the identity of the customer through reliable documentary or non-documentary means. *See, e.g.*, 31 C.F.R. § 1020.220 (CIP requirements for banks).

3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Banks, broker-dealers, mutual funds, FCMs and IB-Cs are prohibited from establishing, maintaining, administering, or managing accounts for foreign shell banks, which are entities effectively unregulated by any prudential supervisor. Shell banks are banks with offshore licences and no physical presence in the country where they are licensed (no offices, employees, or records). Shell banks do not include affiliates of regulated financial institutions (banks that have physical locations and are regulated by a supervisor in the licensing jurisdiction) with offshore licences. 31 C.F.R. § 1010.630.

3.9 What is the criteria for reporting suspicious activity?

Financial institutions and other businesses subject to the AML Program requirement (except Check Cashers, Operators of Credit Card Systems, and Dealers in Precious Metals, Precious Stones, or Jewels) are required to file SARs with FinCEN under the BSA (and for banks, under parallel requirements of their federal functional regulators). SARs are required where the filer "knows, suspects, or has reason to suspect" a transaction conducted or attempted by, at or through the financial institution: (1) involves money laundering; (2) is designed to evade any BSA regulation or requirement; (3) has no business or apparent lawful purpose or is not the sort in which a particular customer would engage; or (4) involves the use of the financial institution to facilitate criminal activity or involves any known or suspected violation of federal criminal law. *See, e.g.*, 31 C.F.R. § 1023.320(c) (SAR requirements for broker-dealers).

Generally, the reporting threshold is $5,000 or more. For banks, if the suspect is unknown, it is $25,000 or more. For MSBs, generally, it is $2,000 or more.

There are very few exceptions to the SAR requirements. For instance, securities broker-dealers and FCMs and IB-Cs are not required to file SARs on violations of securities or future laws by their employees unless they otherwise involve BSA violations, if the information is filed with the SEC, CFTC or their SRO. *See, e.g.*, 31 C.F.R. § 1023.330(c) (SAR exceptions for broker-dealers).

SARs generally must be filed within 30 calendar days after the date of initial detection of the facts that may constitute a basis for filing. Where there are back-end monitoring systems, a reasonable time is allowed to investigate alerts before the 30-day "clock" begins to run. With very few exceptions, there are strict confidentiality requirements pertaining to SARs and the fact that a SAR was or was not filed. *See, e.g.*, 31 C.F.R. § 1020.320(e) (SAR confidentiality for banks). Tipping off would be a crime under the BSA.

There is a safe harbour protection for any business under the BSA statute and their officers, directors, and employees from civil liability for disclosures by filing a SAR. 31 C.F.R. § 1020.320(f); 31 U.S.C. § 5318(g)(3). There is no safe harbour from criminal liability. If a financial institution identified potential suspicious activity, it must decide whether to terminate the customer relationship if further dealing could lead to liability for money laundering. With very rare exceptions, regulators will not direct a financial institution to terminate a customer relationship.

Generally, there is no requirement to notify any government agency that a SAR is being filed. However, FinCEN has issued guidance recommending that prior to closing an account when the financial institution is aware of an ongoing government investigation of the customer, there should be notification to the investigating agency. The agency may request that the financial institution retain the relationship for a period of time to facilitate the investigation.

3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The requirements vary by state. In many, if not most states, the answer is no. Federal legislation to rectify the situation has been proposed several times, but has not been enacted mainly because of the cost and complexity of building a reliable corporate registry with accurate and current ownership information and harmonising state practices.

3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Banks and other financial institutions under the BSA must maintain accurate records relating to funds transfers of $3,000 or more originated by customers and non-customers and verify the identity of non-customers originating funds transfers. The information required to be maintained depends on the role of the financial institution in the payment chain, *i.e.*, originator, intermediary, or beneficiary institution. Financial institutions acting as originator or intermediary financial institutions must cause the information to "travel" to the next financial institution under the BSA Travel Rule. 31 C.F.R. §§ 1010.410 (e) (funds transfer recordkeeping for BSA financial institution and other banks) and 1010.410(f) (the Travel Rule).

3.12 Is ownership of legal entities in the form of bearer shares permitted?

Ownership in the form of bearer shares is not permitted for legal entities organized under the laws of the states of the US. There is no prohibition on providing financial services to entities whose share

are held or authorized to be held in bearer form, but as an AML practice many financial institutions prohibit or restrict relationships with legal entities whose shares are held in bearer form.

3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

There are three requirements with general applicability. As noted, all trades or businesses in the United States, unless designated as financial institutions under the BSA, are subject to cash reporting (Form 8300 reporting). *See* question 3.3. In addition, all persons (individuals and legal persons) are subject to cross-border (CMIR) reporting. *See* question 3.5. Also, under the BSA, all U.S. persons (individuals and legal persons) must report annually all foreign financial accounts valued at $10,000 or more in the aggregate at any point in the previous calendar year if they have an ownership interest in, or (with some exceptions) signatory authority over, the account. This is referred to as the FBAR requirement (Foreign Bank and Financial Accounts Report). 31 C.F.R. § 1010.350.

3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

Not routinely. Under the BSA, however, if there is a demonstrated law enforcement need, FinCEN can impose "geographic targeting" – temporary regulatory requirements for financial institutions or other trades or businesses to file reports or keep records with certain characteristics for a set period of time. 31 C.F.R. § 1010.370. For instance, most recently, there has been a requirement for title insurance companies in certain geographic areas to report cash sales (non-financed sales) of residential real estate purchased by legal entities at given threshold amounts.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

As noted, FinCEN has proposed (but not finalised) regulations that would impose AML Program and SAR requirements on investment advisers registered with the SEC. This would ensure that there would be due diligence on an investor in funds, such as hedge funds and private equity funds, and that the funds transactions would be monitored to detect suspicious activity. 80 Fed. Reg. 52860 (Sept. 1, 2015).

On April 4, 2016, FinCEN issued a Notice of Proposed Rulemaking that proposed amending the definition of broker-dealers under the BSA to include persons registered with the SEC as a "funding portal" to offer or sell crowdfunding. This proposal also has not been finalized.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

As discussed in detail in the most recent FATF mutual evaluation of the United States, there remain a few areas where the United States is not compliant, or is not *fully* in compliance with the FATF recommendations. As noted in question 3.9, the lack of reliable corporate registries is an impediment to financial institutions being able to confirm true beneficial ownership information provided by a customer. The U.S. has not imposed AML requirements on "gatekeepers" consistent with FATF guidance, has not finalised proposed requirements for investment advisers, and has not imposed requirements on real estate agents and trust and company service providers. There has been significant opposition by the legal community to imposing requirements on lawyers as gatekeepers. FinCEN and the federal functional regulators have not specifically addressed the issues of domestic PEPs.

On several occasions since 2008, bills have been introduced in Congress that would require development of a reliable corporate registry with current beneficial ownership information, but the proposals have not been enacted.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The United States was last evaluated by the Financial Action Task Force in 2016. The FATF report is available at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The state and federal statutes cited are available from a number of internet sources. The federal regulations ("C.F.R.") are available at www.ecfr.gov. FinCEN, the federal functional regulators, and SROs all provide access to guidance, advisories, and public enforcement actions through their websites. The FinCEN website is particularly useful with links to statutes, regulations, and Federal Register notices, which provide helpful explanations of proposed and final regulations. *See, e.g.*, FinCEN, www.FINCEN.gov. As noted in question 2.5, the FFIEC manual sets forth extensive guidance for banks.

Joel M. Cohen
Gibson, Dunn & Crutcher LLP
200 Park Avenue, New York
N.Y. 10166
USA

Tel: +1 212 351 2664
Email: jcohen@gibsondunn.com
URL: www.gibsondunn.com

Joel M. Cohen, a trial lawyer and former federal prosecutor, is Co-Chair of Gibson Dunn's White Collar Defense and Investigations Group, and a member of its Securities Litigation, Class Actions and Antitrust Practice Groups. Mr. Cohen has been lead or co-lead counsel in 24 civil and criminal trials in federal and state courts. Mr. Cohen is equally comfortable in leading confidential investigations, managing crises or advocating in court proceedings. Mr. Cohen's experience includes all aspects of FCPA/anticorruption issues, insider trading, securities and financial institution litigation, class actions, sanctions, money laundering and asset recovery, with a particular focus on international disputes and discovery. Mr. Cohen was the prosecutor of Jordan Belfort and Stratton Oakmont, which is the focus of "The Wolf of Wall Street" film by Martin Scorsese. He was an advisor to the OECD in connection with the effort to prohibit corruption in international transactions and was the first Department of Justice legal liaison advisor to the French Ministry of Justice.

Linda Noonan
Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W
Washington, D.C. 20036
USA

Tel: +1 202 887 3595
Email: lnoonan@gibsondunn.com
URL: www.gibsondunn.com

Linda Noonan is Of Counsel in the Washington, D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's Financial Institutions and White Collar Defense and Investigations Practice Groups. She concentrates on Bank Secrecy Act and anti-money laundering compliance and related issues for domestic and multinational banks, securities broker-dealers, insurance companies, casinos, money services businesses, and other financial institutions and a range of financial institution businesses.

Ms. Noonan joined the firm from the U.S. Department of the Treasury, Office of General Counsel, where she had been Senior Counsel for Financial Enforcement. In that capacity, she was the principal legal advisor to Treasury officials on domestic and international money laundering and related financial enforcement issues. During her tenure, she drafted legislation and participated in all major Bank Secrecy Act rulemakings and interpretations and negotiated numerous Bank Secrecy Act civil money penalty cases. She acted as one of the key U.S. delegates to the Financial Action Task Force ("FATF") on money laundering in FATF's early years.

GIBSON DUNN

Gibson, Dunn & Crutcher LLP is a full-service global law firm, with more than 1,200 lawyers in 20 offices worldwide. In addition to 10 locations in major cities throughout the United States, we have 10 in the international financial and legal centers of Beijing, Brussels, Dubai, Frankfurt, Hong Kong, London, Munich, Paris, São Paulo and Singapore. We are recognised for excellent legal service, and our lawyers routinely represent clients in some of the most complex and high-profile matters in the world. We consistently rank among the top law firms in the world in published league tables. Our clients include most of the Fortune 100 companies and nearly half of the Fortune 500 companies.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com