ICLG

The International Comparative Legal Guide to:

Anti-Money Laundering 2018

1st Edition

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

Published by Global Legal Group with contributions from:

Allen & Overy LLP
ANAGNOSTOPOULOS
ASAS LAW
Barnea
BONIFASSI Avocats
C6 an Acuris Company
Castillo Laman Tan Pantaleon & San Jose Law Offices
Chambers of Anuradha Lall
Debevoise & Plimpton
DQ Advocates Limited
Drew & Napier LLC
DSM Avocats à la Cour
Duff & Phelps, LLC
Durrieu Abogados S.C.
EB LEGAL
Encompass
Gibson, Dunn & Crutcher LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Herbert Smith Freehills Germany LLP
JMiles & Co.
Joyce Roysen Advogados
Kellerhals Carrard Zürich KlG
King & Wood Mallesons
Linklaters
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Navigant Consulting
Rato, Ling, Lei & Cortés – Advogados
Rustam Kurmaev & Partners
Shri Singh
WilmerHale
Yamashita, Tsuge and Nimura Law Office

glg
global legal group

global legal group

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

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Senior Editors
Suzie Levy
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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
June 2018

ISBN 978-1-912509-12-6
ISSN 2515-4192

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

PREFACE

We are pleased to provide the preface to *The International Comparative Legal Guide to: Anti-Money Laundering*. This is the inaugural edition on this topic in the ICLG series. It is fitting that Global Legal Group has included this in the series given the importance of the issue and the legal complexities in addressing it.

Money laundering is a global problem of staggering proportions. Over the last thirty 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 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 can be complex, and there are many cross-border compliance issues. Companies that fail to comply with the law and address money laundering risk in their local and international operations face significant legal liability and reputational harm.

Gibson, Dunn & Crutcher LLP joins a group of distinguished colleagues to present several articles on cutting edge issues in AML compliance. This ICLG also includes chapters written by select law firms in 26 countries important to the fight against money laundering, discussing the local AML legal and regulatory/administrative requirements and enforcement environments. Gibson Dunn is pleased to present the chapter on the United States.

As with all ICLG guides, this guide is organised to help the reader understand the legal 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 hope you find this guide useful and encourage you to reach out to the contributors if we can be of further assistance.

Stephanie Brooker & Joel M. Cohen

Gibson, Dunn & Crutcher LLP

Overview of Recent AML Gatekeeper International and U.S. Developments

Stephanie Brooker

Joel M. Cohen

Gibson, Dunn & Crutcher LLP

I Introduction

Money laundering is the process by which a person or entity conceals the existence, nature or source of the proceeds of illegal activity and disguises them to appear legitimate and avoid government detection. Money laundering sustains criminal activity that generates proceeds, facilitating terrorist financing, sanctions violations, and tax evasion, among other illicit activities. Experts disagree on the amount of funds that are laundered annually or even if the scope can be reliably measured.[1] All agree that, despite a recent dramatic increase in international cooperation and law enforcement efforts, the global money laundering problem is one of staggering proportions and continues to threaten stability, including by funding terrorism and nuclear proliferation. The problem persists, in part, because of the cleverness of the wrongdoers and the skill of the professional gatekeepers who are willing to assist them.

The United States and countries around the world have imposed anti-money laundering compliance measures on financial institutions and other businesses to prevent and detect money laundering. The main organisation behind the harmonisation of money laundering countermeasures is the Financial Action Task Force ("FATF"). FATF was established in 1989 as an international body dedicated to "set[ting] standard and promot[ing] effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system".[2] Following the Moscow 1999 Ministerial Conference of the G-8 Countries on Combating Transnational Crime, which recognised the role of "gatekeepers",[3] FATF similarly sharpened its focus on gatekeepers, including lawyers, in facilitating money laundering schemes.[4] Specifically, FATF recognised that "perfectly legitimate functions may . . . be sought out by organised crime groups or the individual criminal" both with the "desire to profit from the expertise of such professionals in setting up schemes that will help to launder criminal proceeds" and in order to cloak themselves with "the veneer of legitimacy".[5] FATF proposed what is known as the "Gatekeeper Initiative" – extending certain anti-money laundering regulations to gatekeeper professionals. This proposal "enlists the support of gatekeepers to combat money laundering and terrorist financing", similar to the way financial institutions have been engaged for many years.[6]

The Gatekeeper Initiative has been met with considerable resistance from the legal community, including in the United States. Lawyers around the globe have emphatically argued that certain anti-money laundering obligations, particularly a mandate that lawyers report suspicious activity relating to their clients, would undermine the relationship of trust and the attorney-client privilege, "the oldest of the privileges for confidential communications known to the common law".[7]

The debate in the United States is far from over. As other countries successfully adopt the Gatekeeper Initiative, as the global threats of drug trafficking, human trafficking, terrorism, and nuclear proliferation intensify, and as long as the United States continues to be an attractive venue for money launderers, it will face pressure to regulate gatekeepers, including attorneys. Because the United States views itself as a leader in eradicating money laundering and terrorist financing, the U.S. legal community may be forced to accept some of the compromises that other jurisdictions have found workable in order to implement the full extent of FATF's recommendations.

This article provides an historical overview of the Gatekeeper issue and discusses recent developments, which are significant, and potential next steps in 2018 and beyond. First, this article will discuss the history of FATF and the Gatekeeper Initiative. It will also address attorney resistance to the Gatekeeper Initiative, focusing especially on criticism of it in the United States. Second, this article will discuss the approaches that major jurisdictions have taken toward gatekeeper regulation in the European Union, the United Kingdom, Hong Kong, Australia, Canada, and the United States. Finally, this article will describe the current climate surrounding gatekeeper regulation, particularly in the United States, including the recently renewed U.S. Congressional interest in enacting gatekeeper legislation and the legal community's response. This article does not take a position on the appropriate course of action in the United States.

II The Financial Action Task Force & the Gatekeeper Initiative

A The Financial Action Task Force

FATF is an international body "that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction".[8] The G-7 countries established FATF at the 1989 Economic Summit Group in Paris.[9] Since then, FATF has spearheaded international anti-money laundering ("AML") efforts. "Its current objectives include 1) revising and clarifying the global standards for combating money laundering and terrorism financing; 2) promoting global implementation of its standards; 3) identifying and responding to new money laundering and terrorist financing threats; and 4) engaging with stakeholders and partners throughout the world".[10]

Most major global financial centers are represented at FATF. It has grown from its G-7 roots to include 35 member jurisdictions (as well as two "Observers").[11] FATF's Forty Recommendations (the "FATF Recommendations" or the "Recommendations"), first adopted in 1990, most recently updated in 2012, and now backed by over 180 countries, embody the framework of FATF's effort to combat money laundering.[12] The Recommendations represent a "comprehensive and consistent framework" to be implemented by each member nation to combat money laundering and terrorist financing.[13] The Forty Recommendations are considered to be the "international standard".[14] Over the years, the initial Recommendations have been refined and expanded to address the changing money laundering landscape, as they were in 2003 to address counter-terrorist financing in the wake of the September 11, 2001 terrorist attacks in the United States.[15]

FATF lacks legal authority with respect to its members. The Recommendations have the effect of "soft law"[16], which are "nonbinding transnational governance standards" promulgated by "substate actors meet[ing] with their peers from other jurisdictions to exchange information, coordinate enforcement, and harmonize the regulatory rules applied at home".[17] Implementation depends on the political will of FATF members, which has been consistently strong in the case of the United States in spite of changing political administrations. FATF seeks enforcement by exerting political pressure on its members, which it does by critiquing them through a mutual evaluation process.[18] Through this evaluation process, FATF "conducts peer reviews of each member on an ongoing basis to assess levels of implementation of the FATF Recommendations, providing an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system".[19] FATF is currently conducting its fourth round of mutual evaluations.[20]

B The Gatekeeper Initiative

Interest in regulating gatekeepers first appeared in the 1996 revisions to the Recommendations. Changes to the original Recommendations included "extending the preventive duties beyond the financial sector".[21] Specifically, the 1996 version suggested that authorities "should consider applying [customer due diligence ("CDD"), recordkeeping, and reporting requirements] to the conduct of financial activities . . . by businesses or professions which are not financial institutions".[22] The list of what was covered by this provision, however, focused on activities (e.g., "money changing"), rather than specific professions.[23] Similarly, the Communique coming out of the Moscow 1999 Ministerial Conference of the G-8 Countries on Combating Transnational Crime recognised the role of gatekeepers.[24]

In 2002, FATF issued a Consultation Paper proposing the expansion of AML regulations to cover non-financial professions that could act as access points or "gatekeepers" to the financial markets for money laundering schemes, whether by serving as financial intermediaries or by providing financial advice.[25] "Gatekeepers" include lawyers, notaries, trust and company service providers, real estate agents, accountants, auditors, as well as other designated non-financial businesses and professions ("DNFBPs") "who assist with transactions involving the movement of money in domestic and international financial systems".[26] The FATF Consultation Paper proposed that certain AML initiatives be extended to these professionals, including CDD, internal compliance training, recordkeeping, filing reports of suspicious activity ("SARs" or "STRs," collectively referred to herein as SAR/STR), and the prohibition against tipping-off, or alerting customers that a SAR/STR involving them is being or has been filed.[27]

Lawyers are seen as especially attractive targets for AML regulation because of their relationship to clients as advisors and confidants.[28] Lawyers' relationships with clients may involve a gatekeeping role in influencing client behavior; for example, lawyers typically advise clients on proper conduct or revise clients' arguments to comply with the duty of candor.[29] Of course, lawyers cannot engage in or perpetuate the client's unlawful conduct and may break attorney-client confidences where necessary (for example, the crime-fraud exception).[30]

Lawyers can, wittingly or unwittingly, play a role in money laundering activity. For example, attorneys can use complex corporate structures, entities, and trusts to mask the source of monies, whether legitimate or criminal.[31] Lawyers' services and their accounts can also be misused in order to "layer[] and conceal[] funds, exploiting the secrecy offered by the legal privilege, and obtaining a veneer of respectability".[32] The Gatekeeper Initiative focuses particularly on unwitting lawyer facilitation of money laundering activities, as intentional facilitation is covered in most countries by criminal statutes.

FATF issued an updated set of Recommendations on June 20, 2003, adopting the Gatekeeper Initiative proposals made in the 2002 Consultation Paper.[33] The revised Recommendations expanded CDD, recordkeeping, and suspicious activity reporting requirements so that they applied to DNFBPs, including lawyers, for financial transactions related to: (1) buying and selling of real estate; (2) managing of client money, securities or other assets; (3) management of bank, savings or securities accounts; (4) organisation of contributions for the creation, operation or management of companies; and (5) creation, operation or management of legal persons or arrangements, and buying and selling of business entities.[34]

The Recommendations stated that the SAR/STR requirement does not apply if the "relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. . . . [i]t is for each country to determine the matters that would fall under legal professional privilege or professional secrecy".[35] However, national legislation incorporating the exception typically has compounded the considerable "uncertainty about the proper scope and application" of the Recommendations' gatekeeper obligations.[36] Although the Recommendations included attorney-client privilege exceptions from suspicious transaction reporting requirements and the no tipping-off rule[37], these exceptions have not forestalled attorney resistance to the Gatekeeper Initiative, as discussed below.

In 2008, FATF published the Risk-Based Approach Guidance for Legal Professionals, similar to a guide that it had previously provided to financial institutions.[38] According to FATF, the purpose of this guidance was to "[s]upport the development of a common understanding of what the risk-based approach involves", "[o]utline the high-level principles involved in applying the risk-based approach", and "[i]ndicate good practice in the design and implementation of the risk-based approach".[39] The guidance acknowledged that this approach is not mandatory but is instead an option to assist lawyers with the efficient allocation of resources, "so that the greatest risks receive the highest attention".[40] FATF also suggested that individual countries "should aim to establish an active dialogue" with attorneys in order to arrive at an effective AML programme.[41]

C Criticism of the Gatekeeper Initiative

The Gatekeeper Initiative has been criticised by many lawyers around the globe. Some have expressed concerns that "FATF incorporated lawyers into its regime of covered parties, but without

meaningful dialogue with the private sector as to causation or appropriate, tailored, and targeted solutions".[42] Others have argued that the costs of applying the Recommendations to lawyers outweigh the benefits.[43] Many have also argued that there is no clear benefit to the Gatekeeper Initiative without stronger evidence that lawyers have been *unknowingly* facilitating money laundering (particularly considering that intentional participants already fall under the ambit of the law).[44] According to this argument, lawyers who intentionally conspire with their clients to launder money would not be deterred by new regulation. Those in opposition have stressed that there are significant costs to upsetting the sanctity of client confidentiality, the independence of the bar, and an attorney's duty of loyalty.[45] Moreover, some have noted that there are substantial monetary costs, particularly for small and solo practices, linked with increased monitoring and tracking.[46]

Despite professional responsibility regimes that differ by country, bar associations around the world have taken up a common cause regarding the effect of the Recommendations.[47] For example, in 2003, bar associations from the United States, Canada, the European Union, Japan, and Switzerland executed the "Joint Statement by the International Legal Profession to the FATF" ("Joint Statement").[48] The Joint Statement highlighted the signatory bar associations' concerns about the consequences of the Recommendations for the principles of the profession.[49] The Joint Statement listed several threatened "core attributes", including client confidentiality, "the independence of the bar from the government," and the duty of loyalty, all of which are "recognised in all [the] legal systems, despite their many differences".[50]

Some in the United States organised legal community opposed the Gatekeeper Initiative. Despite the United States' historic FATF leadership role, FATF's 2006 Third Mutual Evaluation determined that the United States was "non-compliant" with respect to certain Recommendations in part because of the failure to act with respect to gatekeepers.[51] As discussed below, this criticism was repeated in the Fourth Mutual Evaluation of the United States in 2016.[52] The United States has not passed any legislation authorising the direct application of recordkeeping, reporting, and AML compliance programme requirements to attorneys, in contrast to many of its FATF peers.

The American Bar Association ("ABA") has opposed the Gatekeeper Initiative for many years. In February 2002, the ABA organised a Task Force on Gatekeeper Regulation and the Profession ("Task Force") to review FATF and U.S. government proposals and develop positions on the application of anti-money laundering regulations to lawyers.[53] The ABA's policy on the Gatekeeper Initiative, as crafted by the Task Force, remains unchanged today:

> The ABA supports reasonable and necessary domestic and international measures designed to combat money laundering and terrorist financing. However, the Association opposes legislation and regulations that would impose burdensome and intrusive gatekeeper requirements on lawyers, including bills that would subject the legal profession to key anti-money laundering compliance provisions of the Bank Secrecy Act.[54]

The ABA's opposition to AML legislation regulating attorneys is based on a series of arguments. First, the ABA argues that a mandatory reporting scheme for lawyers will interfere with the important separation between the legal profession and the government.[55] The ABA is also opposed to regulations that would affect the "relationship of trust" between attorneys and clients, which it describes as a "bedrock of the U.S. administration of justice and rule of law".[56] According to the ABA, such regulations would undercut an attorney's obligation of confidentiality and duty of loyalty to a client.[57] Even with exceptions for attorney-client privilege, the ABA asserts that clients might decline to seek legal advice if there was a fear that confidences may be broken.[58] Additionally, the ABA raises constitutional concerns related to the Sixth Amendment of the U.S. Constitution's guarantee of effective counsel in criminal proceedings and the Tenth Amendment's reservation of regulatory authority over lawyers to the states.[59] Also, the ABA argues that regulation creates an inherent conflict of interest, raising questions about withdrawal and malpractice risks after reporting a client.[60] Next, the ABA asserts that the vagueness of the term "suspicion" and the complexity of AML regulatory schemes may cause counsel to either over-report or decline representation.[61] Furthermore, the ABA points out that the costs of compliance will likely raise the cost of legal services, and that there is a lack of evidence supporting the benefits of AML legislation applying to attorneys.[62] Finally, the ABA maintains that lawyers are already "subject to extensive ethical requirements and enforcement" and are "obligated under existing ethical rules to counsel their clients to abide by the law".[63]

The ABA's opposition has been consistent with its vigorous defence of the legal professional's adherence to privilege and confidentiality. Skeptics have questioned whether this view has also been partly driven by a commercial motive to maintain the United States as an attractive jurisdiction for investment, incorporation, and the free flow of foreign capital.[64] This investment and incorporation activity, and the attractiveness of businesses being subject to U.S. jurisdiction and wealth being protected by U.S. political and economic stability, is a significant source of legal revenue. As discussed below, the fact that segments in the U.S. legal community appear to have been willing to work with clients with questionable sources of funds may cause pressure to mount to place AML requirements on lawyers.

III Approach in Many Jurisdictions

A Most Countries Have Implemented Gatekeeper Regulations

The majority of FATF member jurisdictions have complied with the FATF Recommendations and imposed gatekeeper regulations on attorneys. As of this writing, the International Bar Association reports that 113 jurisdictions have enacted national legislation that is directly applicable to lawyers.[65]

1 The European Union

The current obligation in the EU's Member States for lawyers to file SARs/STRs arises in relation to transactional work with protections to exempt reporting based on privileged advice or where the facts arise in the conduct of civil or criminal litigation. Enforcement actions against lawyers who have failed to file SARs/STRs or who have breached the no-tipping-off laws are rare but do exist. This regime has come about through the European Union's rigorous implementation of FATF Recommendations, adopting legislative directives to the extent of the Recommendation soon after the issuance of each set of Recommendations and often going beyond FATF standards.[66] Directives are binding on Member States as European Union policy, and each Member State then implements the directive into its national law.[67] The European Union has introduced four directives addressing money laundering and terrorist financing.[68]

In 1991, the European Community adopted the first money laundering directive based on the original FATF Recommendations.[69] The First Directive included obligations only for financial entities.[70] Further revisions to bring the European Union in line with FATF's 1996 revised Recommendations prompted a second AML directive ("Second Directive").[71] The Second Directive was met with considerable resistance from the European legal community,[72] as it

applied to specific DNFBP professions, including lawyers, rather than only certain financial activities as had been the 1996 FATF Recommendations.[73] This was a sticking point in negotiations between the European Council and the European Parliament, which lasted over two years.[74] The delay was primarily due to the European Parliament's concerns regarding the potential impact of the proposed obligations on the right to a fair trial and lawyer-client confidentiality.[75] In the wake of the September 11, 2001 terrorist attacks on the United States, however, a compromise was reached by allowing exemptions from SAR/STR and the no tipping-off rules for attorneys in certain circumstances.[76] The Second Directive was adopted in December 2001.[77]

Another AML directive ("Third Directive") was published in 2005 to implement the 2003 FATF Recommendations.[78] Changes affecting attorneys included the removal of exemptions from the no tipping-off rule and a new requirement that SAR/STR reports filed with bar associations, which was how France, amongst others, had implemented the SAR/STR requirement, be forwarded to financial intelligence units.[79]

While Member States began to implement the Directives, the Second Directive's reporting obligation for attorneys was challenged in Belgian and French courts on the basis that the regulations "contravene rights conferred by the European Convention on Human Rights".[80] As to whether it violated the right to a fair trial, the European Court of Justice ruled in 2007 that it did not because, lawyers only had reporting obligations in relation to a specified class of transactional work, and that as soon as a lawyer engaged in such transactional work was called upon to defend "the client or in representing him before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings", that lawyer would be exempted from the reporting obligation.[81]

On June 25, 2015, the most recent directive ("Fourth Directive") was adopted.[82] The Fourth Directive continues to apply AML regulations to lawyers participating in specified financial transactions.[83] Like the Second and Third Directives, the Fourth Directive recognised an attorney's duty to the client:

> However, where independent members of professions providing legal advice which are legally recognised and controlled, such as lawyers, are ascertaining the legal position of a client or representing a client in legal proceedings, it would not be appropriate under the Directive to put these legal professionals in respect of these activities under an obligation to report suspicions of money laundering. There must be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position for a client. Thus, legal advice remains subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering activities, the legal advice is provided for money laundering purposes, or the lawyer knows that the client is seeking legal advice for money laundering purposes.[84]

European Union Member States were advised to transpose measures of the Fourth Directive by June 26, 2017.[85] To date, all but five Member States have implemented the Fourth Directive.[86]

2 The United Kingdom

Under the Proceeds of Crime Act 2002 (as amended) ("POCA"), lawyers in the United Kingdom who are carrying out transactional, corporate formation, trustee, asset management, and other similar work have a positive reporting obligation if, in the course of that work, they come to know or suspect, or have reasonable grounds to suspect, that another person is involved in money laundering.[87] Lawyers who fail to report under POCA face possible criminal prosecution.[88] The Court of Appeal in R v. Da Silva clarified that the suspicion does not have to be "clear" or "firmly grounded and targeted on specific facts", but there must be a "possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice".[89]

In the United Kingdom, a lawyer must file an "internal" SAR/STR with his or her firm's Money Laundering Reporting Officer ("MLRO"). Failure to so report is a criminal offence by that lawyer.[90] Once the MLRO has received that SAR/STR, and if the MLRO also takes the view that there is sufficient reason to have knowledge or suspicion that a third party is money laundering, then (subject only to a limited number of exceptions) the MLRO commits a criminal offence if he or she does not in turn file a SAR/STR with the UK's National Crime Agency ("NCA").[91] To provide for this possibility, law firms will often have wording about the SAR/STR obligation in their engagement letters. Moreover, section 337 states, in accordance with the EU Second Directive, that the filing of a SAR/STR will not be a breach of a restriction on disclosure, and section 338(4A) provides for immunity from civil liability for SARs/STRs filed in good faith.

POCA contains three key protections for lawyers and clients. First, a lawyer performing other kinds of work for a client – most notably the conduct of litigation – is outside the regime imposing a positive reporting obligation. This was clarified and reinforced by the English Court of Appeal in Bowman v. Fels.[92] The second key protection is that POCA has a statutory privilege regime. Under section 330(6) a lawyer does not have to file a SAR/STR if the information forming the basis of any knowledge or suspicion comes to such lawyer in "privileged circumstances". Privileged circumstances include when information is communicated: (i) by a client (or client representative) in connection with obtaining legal advice; (ii) by a person seeking legal advice (e.g., a prospective client); or (iii) by a person in connection with actual or contemplated legal proceedings (e.g., a witness who may not be a client).[93] As with privilege at common law, there is a "crime/fraud exception" so that if the advice is sought "with the intention of furthering a criminal purpose", the protection then falls away regardless of whether the lawyer knowingly participated in pursuit of the criminal purpose.[94] The final key protection for lawyers is that, in determining whether a lawyer has committed an offence, a court must take into consideration the extent to which that lawyer has complied with approved guidance from the England and Wales Law Society and other similar organisations in other parts of the United Kingdom.[95] A lawyer mistakenly committing an offence while following a regulator's guidance is unlikely to be prosecuted.

The United Kingdom's money laundering laws derive from the European Union directives discussed above.[96] POCA gave effect to the Second Directive, while the Third Directive was implemented in the United Kingdom through regulations in 2007,[97] and the Fourth Directive was mainly implemented through new regulations in 2017.[98]

The extent to which UK and EU policy and legislation continue to be aligned after BREXIT remains to be seen, but it is likely that the key tenets of UK anti-money laundering laws will remain broadly similar to those in place in Europe, at least for the foreseeable future.

3 Hong Kong

Like the EU and the United Kingdom, Hong Kong has enacted AML legislation directly applicable to attorneys. Hong Kong law requires lawyers to report suspicious transactions. Sections 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTRPO") and the Organized and Serious Crimes Ordinance ("OSCO") impose a duty on a person, who knows or suspects that any property represents proceeds of, was used in connection with, or is intended to be used in connection with "drug trafficking" or of an "indictable

offense," to disclose that knowledge or suspicion to an "authorized officer".[99] Failure to disclose is a criminal offence with a penalty of up to three months' imprisonment and a 50,000 HKD fine.[100]

Hong Kong law provides an exception to SAR/STR obligations for legal professional privilege, but it does not provide any for the duty of confidentiality.[101] Section 2(14) of the DTRPO and section 2(18) of the OSCO exempt information subject to the legal professional privilege.[102] While the obligation to report does not override the duty of the legal professional privilege, the Hong Kong courts have held that the legal professional privilege does not protect communications made in order to obtain advice to further a criminal purpose or communications unconnected to the legal advice given or sought; therefore, the obligation to report exists in such circumstances.[103]

FATF's Third Mutual Evaluation Report of Hong Kong, released on July 11, 2008, noted the relative lack of suspicious transaction reporting by DNFBPs.[104] It stated, "[t]here is a very low level of reporting by some [categories of] DNFBPs and complete lack of reporting from others. With the limited exception of the estate agency profession, there are no formal structures in place to monitor [anti-money laundering and combating the financing of terrorism ("AML/CFT")] compliance within the DNFBP sectors", suggesting that the reporting system lacks effectiveness.[105]

There have been recent changes to Hong Kong's AML legislation. Prompted in part by adverse ratings in the last mutual evaluation and the upcoming 2018 evaluation, the Hong Kong legislature recently passed the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018.[106] This amendment, which came into effect on March 1, 2018, extends CDD recordkeeping requirements to solicitors when preparing for or carrying out certain transactions for clients.[107]

B Some Countries Have Been Unable to Implement Gatekeeper Regulations

Many FATF member jurisdictions have not imposed gatekeeper regulations on attorneys. As of this writing, the International Bar Association reports that 35 jurisdictions have enacted legislation that is indirectly applicable to lawyers and seven jurisdictions have yet to enact any national legislation directly or indirectly applicable to lawyers.[108]

1 Australia

Australia considered AML legislation applicable to lawyers around 2007 but did not implement any due to industry opposition.[109] The Law Council of Australia (the "Council") made many of the same arguments as the ABA against such legislation, including that it would threaten "the operation of the doctrine of client legal privilege".[110]

In late 2016, the Australian government proposed a plan to strengthen its AML framework.[111] Specifically, it sought to develop options for applying the SAR/STR regime to lawyers.[112] The proposal was likely a response to FATF's 2015 criticism of Australia for failing to expand AML obligations to DNFBPs.[113] The Council opposed it. In its 2016 updates to its AML guidance for legal practitioners, the Council made clear that a reporting regime remains "fundamentally incompatible" with the role of lawyers and the concept of privilege.[114] In a February 2017 response to the government's proposal, the Council also questioned the efficacy of FATF regulations, particularly considering the "deleterious and unintended consequences" arising out of "further regulation of legal practitioners".[115] It argued that "to date the reduction of financial crime because of a FATF-based response appears to remain elusive".[116] The Council also reiterated that that there remains a dearth of evidence that lawyers are so involved in facilitating money laundering that further regulation is warranted.[117]

Some are skeptical of this argument. Commentators have noted that "a blanket opposition to a reporting obligation based on a perceived lack of evidence that Australian lawyers are involved in money laundering is, at the least, curious".[118] They suggested that the motivation might have been to attract more business – even if it came from money launderers, who can take advantage of Australia's less severe AML regulations paired with its sophisticated financial market.[119]

2 Canada

In 2000, the Canadian Parliament enacted the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "PCMLTFA"), the basis of Canada's AML/CFT regime. Any person or entity subject to the PCMLTFA is required to conduct client identification and verification, maintain records of financial transactions, report proscribed transactions to the government, and establish internal AML/CFT programmes.[120] The PCMLTFA applies to lawyers and law firms when they engage in certain conduct on behalf of a client, including: "receiving or paying funds, other than those received or paid in respect of professional fees, disbursements, expenses or bail" or when "giving instructions in respect to" any of the aforementioned conduct.[121]

Canadian lawyers challenged this legislation after it was enacted.[122] In 2015, after nearly a decade of litigation, the Canadian Supreme Court deemed that certain provisions of the PCMLTFA were a threat to "fundamental justice" by impinging on the attorney-client privilege and a lawyer's duty of commitment to the client.[123] The Canadian Supreme Court thus struck down as unconstitutional the portions of Canada's PCMLTFA that allowed warrantless searches and seizures at lawyers' offices and required lawyers to monitor and report their clients' financial activities to the government.[124]

Former ABA president William C. Hubbard suggested that this opinion has "resonance" for the United States, serving as an important reminder to lawmakers that "regulation of the legal profession has limits".[125] Others were critical of the ruling, noting the gap left in the country's money laundering defenses by "Canada's lawyer loophole".[126] Adam Ross, author of a recent Transparency International report, stated in an interview that, "[t]he law societies claim to have rules in place to prevent money laundering but they are weak, non-transparent and almost never enforced".[127] FATF agreed that these rules are inadequate. Canada's 2016 Mutual Evaluation noted:

> Representatives of the Federation of Law Societies . . . did not demonstrate a proper understanding of [the money laundering/terrorist financing] risks of the legal profession. In particular, they appeared overly confident that the mitigation measures adopted by provincial and territorial law societies (i.e., the prohibition of conducting large cash transactions and the identification and recordkeeping requirements for certain financial transactions performed on behalf of the clients) mitigate the risks.[128]

In a February 2018 report, Canada's Department of Finance recognised lawyers as gatekeepers and referenced a 2015 National Inherent Risk Assessment that found the legal sector to pose a high AML risk.[129] Acknowledging that Canada's Supreme Court struck down the PCMLTFA's application to lawyers, the paper cited to FATF's evaluation, stating that the "lack of inclusion of the legal profession in Canada's AML/ATF framework is a major deficiency that negatively affects Canada's global reputation".[130] Although the paper offered no concrete solutions as to gatekeepers, it affirmatively stated the willingness "to engage Canada's law societies and bar

associations to work with the Government to find solutions" and "to develop constitutionally compliant legislative and regulatory provisions that would subject legal counsel and law firms to the PCMLTFA".[131]

Despite FATF's and the Department of Finance's positions, the law societies in Canada still supported self-regulation. On March 20, 2018, the Federation of Law Societies of Canada submitted comments to the House of Commons Standing Committee on Finance's review of the PCMLTFA.[132] The comments argued that FATF and the Department of Finance "ignore the serious regulatory initiatives of Canada's law societies in this area and the ongoing monitoring of members of the legal profession that law societies engage in including both periodic and risk-based audits".[133] Specifically, the Canadian law societies have also implemented rules prohibiting attorneys from accepting more than $7,500 in cash and requiring client identification and verification.[134] The law societies emphasised their continued efforts, including a "special working group . . . on draft amendments to . . . clarify some of the provisions and add additional obligations," as well as the preparation of "guidance on best practices" and "educational materials for the legal profession" to understand and address risks.[135]

IV The United States History and 2018 Developments

Attempts in the United States to enact AML legislation applicable to attorneys have not succeeded so far. Although proposed legislation has not been enacted, in 2017 and to date in 2018 there has been substantial U.S. legislative activity that might change the outcome.

A Historical Background

Following the 1999 G-8 meetings that resulted in FATF's focus on gatekeepers, the Department of Justice chaired an Interagency Working Group to "examine the responsibilities of professionals, such as lawyers and accountants, with regard to money laundering".[136] Congressional hearings in 2000 outlined a "national strategy to combat money laundering" including "studies on the appropriate role of 'gatekeepers' in the international financial system, such as lawyers and accountants".[137] Testimony by administration officials around the same time highlighted that the executive branch was "aggressively pursuing programs aimed at the lawyers, accountants and auditors who function as 'gatekeepers' to the financial system".[138] The Treasury Deputy Secretary testified to the House Committee on Banking and Financial Services that "[w]hile legal rules properly insulate professional consultations . . . those rules should not create a cover for criminal conduct".[139]

Bills were later introduced that would have covered lawyers engaged in company formation. Beginning in 2007, Senator Carl Levin sponsored a succession of bills requiring the establishment of a reliable corporate registry of beneficial ownership.[140] The proposed legislation would have also made formation agents, which appeared to cover some lawyers, liable for providing false information about beneficial ownership.[141] The legislation also sought to expand the definition of "financial institution" under the Bank Secrecy Act ("BSA")[142] to include "any person involved in forming a corporation, limited liability company, partnership, trust, or other legal entity".[143]

In response to these efforts, the ABA argued that oversight of the state supreme courts, the threat of prosecution, and voluntary guidance are sufficient to detect and prevent unwitting facilitation of money laundering.[144] The ABA pointed out that lawyers are also bound by the ABA Model Rules of Professional Conduct, which have been adopted by most jurisdictions.[145] Several Model Rules, the ABA argued, serve similar functions as FATF's Recommendations in detecting and preventing money laundering. For example, "the confluence of the mandates in Rules 1.1, 1.2(d), and 8.4 should result in the lawyer obtaining substantial client information and underscoring his duty to refrain from facilitating any illegal conduct the client may wish to carry out".[146]

Furthermore, the ABA reasoned, the most effective way to combat unwitting attorney facilitation of money laundering is to educate lawyers.[147] The ABA proposed that lawyers would be more aware if they better understood the ways in which their services might be taken advantage of by criminals.[148] To this end, in 2010, the ABA implemented the Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing ("Good Practices Guidance") to "serve as a resource that lawyers can use in developing their own voluntary risk-based approaches" to CDD and monitoring procedures to detect potentially suspicious transactions.[149] The ABA's intention was that the Good Practices Guidance would encourage vigilance and prove legislation of attorneys to be unnecessary.[150] Critics have argued that the Good Practices Guidance is not sufficient. Legal counsel for Global Financial Integrity noted that, "[i]f you went out and asked lawyers, 'Have you ever heard of these voluntary guidelines?' 99 percent will say they have never heard of them".[151] One attorney in Washington, D.C. said that "[t]he ABA voluntary guidance is a joke because there are no consequences, unless you're prosecuted, and that happens once every five years".[152]

B Current State of Play

In December 2016, FATF issued its first Mutual Evaluation Report of the United States in a decade.[153] Although the United States was deemed largely compliant, the 2016 Report noted that the U.S. regulatory framework had significant gaps. Areas of non-compliance included the absence of federal beneficial ownership reporting requirements for all domestic companies and a lack of AML/CFT requirements for most DNFBPs, including lawyers.[154] According to one prominent practitioner commenting at the time, "[t]he noncompliant rating issued by FATF for the legal profession will undoubtedly stir increased federal legislative and regulatory action seeking to impose AML/CFT obligations on U.S. lawyers".[155]

In addition to the release of the Mutual Evaluation Report, recent high-profile events have suggested that lawyers can be facilitators of money laundering and that there may be holes in the U.S. AML regime with respect to gatekeepers generally. In 2015, Global Witness, an international non-governmental organisation, whose mission is to fight global corruption, conducted a sting operation on New York lawyers.[156] The investigation eventually aired on CBS's *60 Minutes* (a prominent U.S. television news programme) in February 2016. As part of the exposé, an undercover investigator approached 13 lawyers, posing as an advisor to an African minister and claiming the minister had accumulated millions of dollars helping companies receive mining concessions in his country.[157] He sought advice on moving the funds in ways that may have aroused suspicions – suggesting that the minister wanted to purchase a townhouse, a jet, or a yacht through corporate structures that did not connect his name to the purchases.[158] According to Global Witness, all but one of the 13 lawyers approached appeared to provide at least preliminary advice on moving suspect funds into the United States.[159]

Less than a year later, two prominent incidents generated substantial global interest in gatekeeper regulation and exposed the potential

role of segments of the legal profession in money laundering. First were the leaks of the Panama Papers in April 2016 and the Paradise Papers in 2017, both of which illustrated the extent to which law firms may have been involved in concealing criminal proceeds and fostering tax evasion.[160] Just a few months later, the United States Department of Justice filed a civil asset forfeiture case involving stolen funds from the Malaysian sovereign wealth fund, allegedly moved through a trust account at a major U.S. law firm.[161]

These events reinvigorated some lawmakers to hold hearings and reintroduce legislation mandating the collection of beneficial ownership information and extending BSA requirements to attorneys engaged in business formation activities.[162] For example, on February 3, 2016, Senators Sheldon Whitehouse and Dianne Feinstein and Representatives Carolyn Maloney and Peter King reintroduced the Incorporation Transparency and Law Enforcement Assistance Act[163], a redux of earlier proposed prior beneficial ownership bills, referencing the Global Witness investigation in supporting press releases.[164]

Over a year later, on June 28, 2017, Senator Whitehouse (along with Senators Feinstein and Charles Grassley) introduced a very similar bill, the True Incorporation Transparency for Law Enforcement ("TITLE") Act.[165] Citing recent events, Senator Whitehouse explained that the proposed legislation "would address corporate transparency loopholes exposed by the Panama Papers" by "extend[ing] money laundering due diligence requirements that currently apply to banks to professionals that help form business entities".[166] The same day, Representatives Maloney and King introduced the similar Corporate Transparency Act of 2017[167], also citing to the Panama Papers incident.[168] Senators Ron Wyden and Marco Rubio introduced a Senate version of the Corporate Transparency Act of 2017 on August 2, 2017.[169]

Similar to prior proposed legislation, these bills seek to apply the duty of collecting, maintaining, and reporting beneficial ownership information to law firms, lawyers, and other "formation agents" who assist clients in forming corporate entities.[170] These five recent bills cite FATF's criticism of the United States for failing to meet standards for the collection of beneficial ownership information and the need to "level the playing field" of states' formation and incorporation rules.[171] Significantly, all the bills provide civil and criminal penalties – including imprisonment – which would be applicable to formation agents for "knowingly failing to obtain or maintain credible, legible, and updated beneficial ownership information".[172]

Notably, the bills, along with legislation introduced on April 5, 2017 by Senator Whitehouse and Representative Lloyd Doggett[173], would also bring attorneys who act as formation agents (persons engaged in the business of forming corporations and limited liability companies) under BSA anti-money laundering requirements. Specifically, the bills would amend 31 U.S.C. § 5312(a)(2) to include formation agents in the definition of "financial institution" under the BSA and would instruct the Secretary of the Treasury to publish BSA regulations requiring formation agents "to establish anti-money laundering programs" under 31 U.S.C. § 5318(h) (including, at a minimum, the development of policies, the designation of a compliance officer, ongoing employee training, and independent audit functions).[174] Once designated as a financial institution under the BSA regulations, the Department of the Treasury could exercise its authority under the BSA to impose additional BSA requirements on formation agents, including the requirement to report suspicious activity. It is noteworthy that these provisions do not cover all the activities of lawyers that are the subject of the FATF Gatekeeper Initiative.[175]

In 2016, the Obama administration, also citing the Panama Papers leaks, supported these efforts to build a reliable corporate registry with beneficial ownership information, even drafting their own version of the legislation; notably, it did not include a gatekeeper provision.[176]

It remains to be seen whether the Congressional momentum will continue on this issue and whether the Trump administration will encourage or support gatekeeper legislation. Congressional hearings in late 2017 and early 2018 indicate that the issue remains important for lawmakers and stakeholders alike. At a November 29, 2017 hearing before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, Stefanie Ostfeld of Global Witness testified that "while banks serve as the frontline of defense . . . . [t]hose seeking to move suspect funds utilize the services of a wide range of professional gatekeepers," including lawyers.[177] Ostfeld further testified that, in compliance with international standards and FATF's assessment, the United States should subject formation agents to AML obligations, including customer due diligence and recordkeeping requirements.[178]

On January 9 and January 17, 2018, the Senate Committee on Banking, Housing, and Urban Affairs held hearings on BSA reforms and enforcement. Also citing to FATF's findings and the Panama Papers incident, Heather Lowe of Global Financial Integrity, testified before the Committee that "[a]lthough banks serve as an immediate gateway . . . [o]ther actors handle large sums of money, such as . . . lawyers [and] must also take responsibility for knowing with whom they are doing business and guard against their services being used to launder dirty money".[179]

At a February 6, 2018 hearing before the Senate Judiciary Committee, Senator Grassley, citing to the Panama Papers incident, again pushed for an improvement in beneficial ownership transparency.[180] Referencing the Global Witness investigation, he stated that "[t] he lawyers who help set up these companies are complicit," concluding that "[a]lmost all of the lawyers happily agreed [to set up companies to hide assets], eager to generate fees".[181] Senator Grassley chastised the ABA for "defend[ing] these practices".[182] Gary Kalman, Executive Director of the Financial Accountability and Transparency Coalition, testified at the hearing about the problem of individuals using "front people," including attorneys, to file paperwork under the attorney's name, "even though the attorney has no control or economic stake in the company".[183] Kalman also rebuffed the ABA's complaints, arguing that the TITLE Act's "intentionality standard is narrower—with greater protections for those who might make a mistake—than the standard in the American Bar Association's guidelines to lawyers for handling potential anti-money laundering situations".[184] And, at the same hearing, Chip Poncy, President of the Financial Integrity Network, testified that attorney-client privilege concerns by law firms "should not be used to shield company formation agents—including law firms that wish to engage in such activity—from implementing AML/CFT program requirements".[185] He continued that these procedures have the added benefit of protecting "the integrity of company formation agents, including law firms . . . . Any such legitimate firm . . . should agree".[186] Significantly, however, none of this proposed legislation has been referred out of committee.

The ABA has continued to oppose the lawmakers' efforts.[187] In a May 24, 2016 letter, then-ABA President Paulette Brown reiterated that these efforts would "undermine the attorney-client privilege, the confidential lawyer-client relationship, and the state court regulation of the legal profession".[188] There is some movement, however, within the ABA to adopt a model rule that would obligate attorneys to perform risk-based due diligence on prospective clients or matters; significantly, such a rule would subject non-compliant attorneys to discipline by the state bar rather than by the government.[189] On November 27, 2017, the ABA also submitted a letter to the House Committee on Financial Services, opposing legislation "that

would impose burdensome and intrusive regulations on millions of small businesses and their lawyers" by requiring them "to submit extensive information about the companies' 'beneficial owners' to the Treasury Department's Financial Crimes Enforcement Network (FinCEN)".[190]

Most recently, the ABA submitted a letter in connection with the Senate Judiciary Committee's February 6, 2018 hearing on "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency". The ABA maintained its position that this (and similar) legislation "would undermine the attorney-client privilege and impose burdensome and intrusive regulations on millions of small businesses, their agents, and the states".[191] Specifically, ABA President Hilarie Bass argued that the legislation's reporting requirements "would compel lawyers to report certain privileged or confidential client information to government authorities," which is "plainly inconsistent with their ethical duties and obligations".[192] Consistent with the ABA's historical position, Bass wrote that these reporting requirements are also unnecessary because "the federal government, financial institutions, and the legal profession have developed other tools and taken other steps," including the ABA's Good Practices Guidance, which "are much more effective and practical".[193]

The force of FATF soft law cannot be underestimated even though the next Mutual Evaluation is not until 2026. The United States has enacted legislation and promulgated BSA regulations responsive to the FATF recommendations for over 20 years. Criticism from the first Mutual Evaluation eventually led to the imposition of anti-money laundering requirements on the insurance industry, after many years of consideration. Similarly, FATF criticism arguably inspired the BSA customer due diligence regulations that will come into force on May 11, 2018. External events can also drive action, just as the tragedies of September 11, 2011 led to the PATRIOT Act, which enacted many BSA provisions that had been pending in Congress for several years. The continued pressure in the United States to enact anti-money laundering requirements on gatekeepers and fulfill its commitment to FATF may eventually override the opposing arguments and concerns.

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Linda Noonan, Laura Plack, and Ian Sprague in the preparation of this chapter.

Endnotes

1. *See* U.N. Office on Drugs & Crime, *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes: Research Report* 15 (Oct. 2011).
2. *Who We Are*, Fin. Action Task Force, http://www.fatf-gafi.org/about/ (last visited Mar. 21, 2018) [hereinafter *Who We Are*].
3. Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, Russ., Oct. 19–20, 1999, *Communiqué* ¶ 32, https://www.justice.gov/sites/default/files/ag/legacy/2004/06/09/99MoscowCommunique.pdf [hereinafter *Communiqué*].
4. *See* Kevin L. Shepherd, *Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transactional Lawyers*, 43 Real Prop. Tr. & Est. L.J. 607, 610–11 (2009).
5. Fin. Action Task Force [FATF], *Report on Money Laundering Typologies* 24 (2003–2004), http://www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf.
6. Shepherd, *supra* note 4, at 611.
7. *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).
8. FATF, *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* at intro. (Feb. 2013), http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf.
9. *History of the FATF*, Fin. Action Task Force, http://www.fatf-gafi.org/about/historyofthefatf/ (last visited Mar. 21, 2018) [hereinafter *History of the FATF*].
10. Laurel S. Terry, *An Introduction to the Financial Action Task Force and Its 2008 Lawyer Guidance*, 2010 J. Prof. Law. 3, 6 (2010).
11. *FATF Members and Observers*, Fin. Action Task Force, http://www.fatf-gafi.org/about/membersandobservers/#d.en.3147 (last visited Mar. 21, 2018).
12. *History of the FATF*, *supra* note 9; FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* 12 (Feb. 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [hereinafter *2012 Recommendations*].
13. *2012 Recommendations*, *supra* note 12, at 6.
14. *Id.*
15. *Id.*
16. Terry, *supra* note 10, at 9.
17. Jean Galbraith & David Zaring, *Soft Law as Foreign Relations Law*, 99 Cornell L. Rev. 735, 745 (2014).
18. *See Topic: Mutual Evaluations*, Fin. Action Task Force, http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate) (last visited Mar. 21, 2018).
19. *Id.*
20. *See* FATF, *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations* 3 (Nov. 2017), http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF-4th-Round-Procedures.pdf.
21. Valsamis Mitsilegas & Bill Gilmore, *The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in Light of Evolving Global Standards*, 56 Int'l & Comp. L.Q. 119, 122 (2007).
22. FATF, *The Forty Recommendations* ¶ 9 (1996), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf [hereinafter *1996 Recommendations*].
23. *Id.* ¶ 8.
24. *Communiqué*, *supra* note 3, ¶ 32.
25. *See* Danielle Jasmin Kirby, Note, *The European Union's Gatekeeper Initiative: The European Union Enlists Lawyers in the Fight Against Money Laundering and Terrorist Financing*, 37 Hofstra L. Rev. 261, 272–73 (2008).
26. Am. Bar Ass'n, Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing 1 (2010), https://www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_taskforce_gtfgoodpracticesguidance.authcheckdam.pdf [hereinafter Good Practices Guidance].
27. Kirby, *supra* note 25, at 273.
28. Jack P. Sahl, *Lawyer Ethics and the Financial Action Task Force: A Call to Action*, 59 N.Y. L. Sch. L. Rev. 457, 473 (2014–15).
29. *See, e.g.*, Model Rules of Prof'l Conduct R. 3.3. *See generally* Fred Zacharias, *Lawyers as Gatekeepers*, 41 San Diego L. Rev. 1387, 1390 (2004).
30. *See* Model Rules of Prof'l Conduct R. 1.6.
31. Patricia Shaughnessy, *The New EU Money Laundering Directive: Lawyers as Gatekeepers and Whistle-Blowers*, 34 L. & Pol'y Int'l Bus. 25, 30 (2002).

32. *Id.*
33. *See* FATF, *The Forty Recommendations* 5–6 (June 20, 2003), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf [hereinafter *2003 Recommendations*]; *see also* Kirby, *supra* note 25, at 273–74.
34. *2003 Recommendations*, *supra* note 33, at 5–6.
35. *2012 Recommendations*, *supra* note 12, at 82; *see also 2003 Recommendations*, *supra* note 33, at 6.
36. Terry, *supra* note 10, at 12.
37. *2003 Recommendations*, *supra* note 33, at 6.
38. FATF, *RBA Guidance for Legal Professionals* 4 (Oct. 23, 2008), http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf.
39. *Id.*
40. *Id.* at 5, 8.
41. *Id.* at 5.
42. *See, e.g.*, Shepherd, *supra* note 4, at 623.
43. *See, e.g.*, Terry, *supra* note 10, at 12.
44. *See, e.g.,* Am. Bar Ass'n, Task Force on Gatekeeper Regulation and the Profession, Report to the House of Delegates 13 (2003), https://www.americanbar.org/content/dam/aba/directories/policy/2003_my_104.authcheckdam.pdf [hereinafter Report to the House of Delegates]; Terry, *supra* note 10, at 12.
45. Report to the House of Delegates, *supra* note 44, at 8-13; Terry, *supra* note 10, at 12.
46. Report to the House of Delegates, *supra* note 44, at 13; The Law Society of England and Wales, The Costs And Benefits Of Anti-Money Laundering Compliance For Solicitors: Response By The Law Society Of England And Wales To The Call For Evidence In The Review Of The Money Laundering Regulations 2007 24-27 (2009), http://www.lawsociety.org.uk/support-services/risk-compliance/anti-money-laundering/documents/law-society-response-to-the-hm-treasury-money-laundering-review-2009/.
47. Terry, *supra* note 10, at 40–41.
48. Joint Statement by the International Legal Profession on the Fight Against Money-Laundering (Apr. 3, 2003), http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/ANTI_MONEY_LAUNDERING/AML_Position_papers/EN_AML_20030403_Joint_statement_by_the_international_legal_profession_to_the_FATF_on_the_fight_against_money-laundering.pdf [hereinafter Joint Statement]; *see also* Terry, *supra* note 10, at 41.
49. *See generally* Joint Statement, *supra* note 48; *see also* Terry, *supra* note 10, at 40–41.
50. Joint Statement, *supra* note 48, ¶ 3.
51. FATF, *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: United States of America* 210-11, 300 (June 23, 2006), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf [hereinafter *U.S. Third Mutual Evaluation*].
52. FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: United States Mutual Evaluation Report* 222-26 (Dec. 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf [hereinafter *U.S. Fourth Mutual Evaluation*].
53. *Task Force on Gatekeeper Regulation and the Profession*, Am. Bar Ass'n, https://www.americanbar.org/groups/criminal_justice/gatekeeper.html (last visited Mar. 21, 2018).
54. *Gatekeeper Regulations on Lawyers*, Am. Bar Ass'n, https://www.americanbar.org/advocacy/governmental_legislative_work/priorities_policy/independence_of_the_legal_profession/bank_secrecy_act.html/ (last visited Mar. 21, 2018).
55. Report to the House of Delegates, *supra* note 44, at 7–9.
56. *Id.* at 7, 9.
57. *Id.* at 9–10.
58. *Id.* at 10.
59. *Id.* at 11.
60. *Id.* at 12.
61. *Id.*
62. *Id.* at 7, 13.
63. *Id.* at 8.
64. This brings into question the U.S. non-compliance with another FATF recommendation to build a corporate registry that authorities can access and use to evaluate beneficial ownership. *See U.S. Fourth Mutual Evaluation*, *supra* note 52 (finding the United States non-compliant with FATF's recommendation regarding the maintenance of beneficial ownership information because of "unsatisfactory measures for ensuring that there is adequate, accurate and updated information" on beneficial owners available to the authorities). According to a World Bank survey, the United States is the most sought-after destination for corrupt government officials to incorporate a company. Emile Van Der Does De Willebois, et al., The World Bank, The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets And What to Do About It 121 (2011), https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf. A 2012 study found that the United States is the second easiest place (after Kenya) to create anonymously owned companies. Kevin Wack, *Why Big Banks Want a Ban on Anonymous Shell Companies*, Am. Banker (Mar. 6, 2017), https://www.americanbanker.com/news/why-big-banks-want-a-ban-on-anonymous-shell-companies; *see also* Ben Judah, Hudson Institute, The Kleptocracy Curse: Rethinking Containment 23 (2016) (acknowledging that "American bankers, accountants, and lawyers are also operating as enablers"); Casey Michel, *The U.S. Is a Good Place for Bad People to Stash Their Money*, The Atlantic (July 13, 2017), https://www.theatlantic.com/business/archive/2017/07/us-anonymous-shell-companies/531996/ (describing the ease with which one can establish an anonymous shell company in the United States).
65. Int'l Bar Ass'n, *Global Chart*, Anti-Money Laundering Forum, https://www.anti-moneylaundering.org/globalchart.aspx (last visited Mar. 22, 2018).
66. Colin Tyre, *Anti-Money Laundering Legislation: Implementation of the FATF Forty Recommendations in the European Union*, 2010 J. Prof. Law. 69, 69–70 (2010); Mitsilegas, *supra* note 21, at 120.
67. Kirby, *supra* note 25, at 276–77 (citing Ralph H. Folsom, Principles of European Union Law 30–31 (2005)).
68. *See generally* Council Directive 2015/849, of the European Parliament and of the Council of May 20, 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 (EU) [hereinafter Fourth Directive].
69. *See* Council Directive 91/308, of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering, 1991 O.J. (L 166) 77 (EC) [hereinafter First Directive]; Mitsilegas, *supra* note 21, at 119–20.
70. Mitsilegas, *supra* note 21, at 120.
71. *See* Council Directive 2001/97 of the European Parliament and of the Council of 4 Dec. 2001 amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering, 2001 O.J. (L 344) 76 (EC) [hereinafter Second Directive]; Kirby, *supra* note 25, at 282.
72. Tyre, *supra* note 66, at 71.

73. *See 1996 Recommendations*, *supra* note 22, ¶ 9; Second Directive, *supra* note 71, art. 1.; *see also* Mitsilegas, *supra* note 21, at 123.
74. Mitsilegas, *supra* note 21, at 123.
75. *Id.*; Kirby, *supra* note 25, at 283.
76. Mitsilegas, *supra* note 21, at 123-24 (citing Second Directive, *supra* note 71, ¶ 5, 7); Tyre, *supra* note 66, at 71; Kirby, *supra* note 25, at 283.
77. Second Directive, *supra* note 71.
78. Council Directive 2005/60/EC of the European Parliament and of the Council of 26 Oct. 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, 2005 O.J. (L 309) 15 (EU) [hereinafter Third Directive]; Kirby, *supra* note 25, at 289.
79. Third Directive, *supra* note 78, arts. 23, 28; Mitsilegas, *supra* note 21, at 127–28.
80. Tyre, *supra* note 66, at 72.
81. Case C-305/05, Ordre des barreaux francophones et germanophone and others v. Counseil des ministres, 2007 E.C.R. I-5308, ¶¶ 33-34. A separate challenge to the reporting requirements was made alleging infringement of the right to privacy under the European Convention of Human Rights. The European Court of Human Rights confirmed that the obligation to report "does not constitute disproportionate interference with the professional privilege of lawyers". *See* Michaud v. France (Application 12323/11), especially paragraph 131.
82. Fourth Directive, *supra* note 68.
83. *Id.* art. 2.
84. *Id.* at 77.
85. Press Release, EC, Strengthened EU Rules to Tackle Money Laundering, Tax Avoidance, and Terrorism Financing Enter into Force (June 26, 2017), http://europa.eu/rapid/press-release_IP-17-1732_en.htm.
86. *Document 32015LO849, National Transposition*, Eur-Lex, http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32015L0849 (last visited Apr. 18, 2018). The five outstanding Member States are Ireland, Greece, Netherlands, Poland, and Romania.
87. Proceeds of Crime Act 2002, c. 29 § 330 (UK), as read with Schedule 9, paragraphs 1(n) and 1(o).
88. POCA §§ 330, 331. For a recent prosecution, see R v. Neil Bolton (unreported, T20160199) where a solicitor was sentenced to nine months' jail for failing to file necessary SARs/STRs.
89. R v. Da Silva [2006] EWCA Crim 1654.
90. POCA § 330.
91. POCA § 331.
92. Bowman v. Fels [2005] 1 WLR 3083; [2005] EWCA Civ 226.
93. POCA § 330(10).
94. POCA § 330(11).
95. POCA § 331(7) with POCA Schedule 9, paragraph 4(2).
96. Terry, *supra* note 10, at 29.
97. Kirby, *supra* note 25, at 304.
98. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (S.I. 692/2017) (UK).
99. Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 § 25A (H.K.); Organized and Serious Crimes Ordinance, Cap. 455 § 25A (H.K.); *see also Guideline No. 3.3.2: Drug Trafficking (Recovery of Proceeds)(Amendment) Ordinance 1995, Organized and Serious Crimes (Amendment) Ordinance 1995*, H.K. Monetary Auth. (Aug. 1, 2011), http://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/guidelines/guide_332b.shtml; H.K. Securities and Futures Comm'n, Guideline on Anti-Money Laundering and Counter-Terrorist Financing § 1.24 (Mar. 1, 2018), http://www.sfc.hk/web/EN/rules-and-standards/codes-and-guidelines/guidelines/ [hereinafter SFC Guideline].
100. Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 § 25A (H.K.); Organized and Serious Crimes Ordinance, Cap. 455 § 25A (H.K.); *see also* SFC Guideline, *supra* note 99, § 1.24.
101. Gavin Lewis & Sarah Martin, *Privilege: Hong Kong*, Global Investigations Rev. (Oct. 4, 2017), http://globalinvestigationsreview.com/jurisdiction/1000393/hong-kong.
102. Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 § 2(14) (H.K.); Organized and Serious Crimes Ordinance, Cap. 455 § 2(18) (H.K.).
103. *See* Pang Yiu Hung Robert v. Commissioner of Police and Another [2002] 4 H.K.C. 579; *see also* R v. Cox and Railton [1884] 1 Q.B.D. 153.
104. FATF, *Third Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism, Hong Kong, China*, ix (July 11, 2008), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Hong%20Kong%20full.pdf.
105. *Id.*
106. Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018, Cap. 615; *see also* Press Release, The Government of Hong Kong Special Administrative Region, Gazettal of Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018 and Companies (Amendment) Ordinance 2018 (Feb. 2, 2018), http://www.info.gov.hk/gia/general/201802/02/P2018020200666.htm; Letter from Meena Datwani, Exec. Dir., H.K. Monetary Auth., to Chief Executives at All Authorized Institutions (June 23, 2017), http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20170623e2.pdf.
107. Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018, Cap. 615; *see also* Legislative Council Brief, Anti-Money Laundering and Counter-Terrorist Financing (Financing Institutions) Ordinance, https://www.legco.gov.hk/yr16-17/english/bills/brief/b201706231_brf.pdf.
108. *Global Chart*, *supra* note 65.
109. *See* Anita Clifford, *The Gate is Open: The Need to Expand the AML Suspicious Activity Reporting Regime in Australia*, Bright Line Law: BLL Portal (Dec. 5, 2016), https://www.brightlinelaw.co.uk/White-Collar-Crime-Portal/The-gate-is-open-the-need-to-expand-the-aml-suspicious-activity-reporting-regime-in-australia.html.
110. Law Council of Austl., Response to Consultation Paper: Legal Practitioners and Conveyancers: A Model for Regulation Under Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime 6 (2017), https://www.lawcouncil.asn.au/resources/submissions/a-model-for-regulation-under-australia-s-anti-money-laundering-and-counter-terrorism-financing-regime [hereinafter Response to Consultation Paper].
111. Austl. Gov't Att'y-Gen.'s Dep't, Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations (2016), https://www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf.
112. *Id.* at 28–35.
113. *Id.* at 30; Clifford, *supra* note 109; *see also* FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report* 7 (Apr. 2015), http://

www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf.

114. Law Council of Austl., Anti-Money Laundering Guide for Legal Practitioners 17 (2016), https://www.lawcouncil.asn.au/docs/94749cb5-3c56-e711-93fb-005056be13b5/1601-Policy-Guideline-Anti-Money-Laundering-Guide-for-Legal-Practitioners.pdf.
115. Response to Consultation Paper, *supra* note 110, at 5-6.
116. *Id.* at 5.
117. *Id.* at 7.
118. Clifford, *supra* note 109.
119. *Id.*
120. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17., ss. 6, 7 (Can.) [hereinafter PCMLTFA].
121. SOR/2002-184, ss. 33.3-33.5 (Can.) (regulations applying parts of the PCMLTFA to lawyers).
122. Terry, *supra* note 10, at 34.
123. *Canada (Attorney General) v. Federation of Law Societies of Canada*, [2015] 1 S.C.R. 401, 409–11 (Can.); *see also Advocacy on Behalf of Canada's Law Societies*, Fed'n of Law Soc'y of Can., https://flsc.ca/national-initiatives/advocacy-on-behalf-of-canadas-law-societies/ (last visited Mar. 28, 2018).
124. Canada (Attorney General) v. Federation of Law Societies of Canada, 1 S.C.R. at 410-11.
125. *William C. Hubbard, Opinion, Confidentiality Versus Money-Laundering Laws*, Nat'l L. J. (Mar. 10, 2015), https://www.nelsonmullins.com/DocumentDepot/Op%20Ed%20Confidentiality%20Versus%20Money%20Laundering%20Laws%20_%20National%20Law%20Journal.pdf.
126. Sam Cooper, *Battle over Lawyers' Money-Laundering Loophole Shapes Up in B.C.*, Vancouver Sun (Mar. 1, 2017), http://vancouversun.com/news/national/b-c-a-battleground-for-lawyer-loophole-cases.
127. *Id.*
128. FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Canada Mutual Evaluation Report* 81 (Sept. 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf (internal citations omitted).
129. Dep't of Fin. Canada, Reviewing Canada's Anti-Money Laundering & Anti-Terrorist Financing Regime 20 (2018), https://www.fin.gc.ca/activty/consult/amlatfr-rpcfa-eng.pdf.
130. *Id.* at 21.
131. *Id.*
132. Fed'n of L. Soc'y of Can., Submission of the Federation of Law Societies of Canada to the House of Commons Standing Committee on Finance re Statutory Review of the Proceeds of Crime (Money Laundering) and Terrorist Finance Act (2018), https://flsc.ca/wp-content/uploads/2018/03/MONEYLaunderENMarch2018F.pdf.
133. *Id.* at 3.
134. *Id.* at 2.
135. *Id.* at 3–4.
136. U.S. Dep't of State, *Money Laundering and Financial Crimes*, https://2009-2017.state.gov/j/inl/rls/nrcrpt/2000/959.htm (last visited Mar. 22, 2018); *see also* Report to the House of Delegates, *supra* note 44, at 6.
137. *Hearing on Combating Money Laundering Before the Subcomm. on Crim. J., Drug Policy, and Human Resources of the H. Comm. on Gov't Reform*, 106th Cong. 4–5 (2000) (statement of Rep. John L. Mica).
138. *Hearing on Offshore Money Laundering Before the H. Comm. on Banking and Fin. Servs.*, 106th Cong. 30 (2000) (statement of Stuart Eizenstat, Deputy Secretary, U.S. Dep't of the Treasury).
139. *Id.*
140. *See, e.g.*, Incorporation Transparency and Law Enforcement Assistance Act, H.R. 3331, 113th Cong. (2013); Incorporation Transparency and Law Enforcement Assistance Act, S. 2956, 110th Cong. (2008).
141. *E.g.*, S. 2956 § 3.
142. The Bank Secrecy Act or BSA authorises the Secretary of the Treasury to impose recordkeeping, reporting and anti-money laundering programme requirements on financial institutions and other businesses. The BSA is not generally self-executing but its requirements must be implemented through regulation. 31 U.S.C. § 5311 *et seq.* (BSA statute) and 31 CFR Part X (implementing regulations).
143. *E.g.*, S. 2956 § 4.
144. *See* David Voreacos, *Malaysian Fund Pilfering Scheme Shines Light on Law Firm's Role*, Bloomberg (July 22, 2016), https://www.bloomberg.com/news/articles/2016-07-22/malaysian-fund-pilfering-claim-shines-light-on-law-firm-s-role.
145. Jack P. Stahl, *Lawyer Ethics and the Financial Action Task Force: A Call to Action*, 59 N.Y.L. Sch. L. Rev. 457, 475 (2014).
146. *Id.* at 478.
147. Laurel S. Terry, *U.S. Legal Profession Efforts to Combat Money Laundering and Terrorist Financing*, 59 N.Y.L. Sch. L. Rev. 487, 502 (2014).
148. *Id.*
149. Good Practices Guidance, *supra* note 26, at 7; *see also id.* at 8–9.
150. Letter from Stephen N. Zack, Pres., Am. Bar Ass'n, to State Bar Presidents (Apr. 8, 2011) ("In our view, the Voluntary Guidance is the most effective means of both combating money laundering and avoiding the passage of federal legislation or adoption of rules that would impose unnecessary, costly, and burdensome new regulations on lawyers and the legal profession and adversely affect the clients that we serve".); *see also* Michael A. Lindenberger, *Into the Breach: Voluntary Compliance on Money Laundering Gets a Boost from the ABA and Treasury*, Am. Bar Ass'n J. (Oct. 2011), http://www.abajournal.com/magazine/article/into_the_breach_voluntary_compliance_on_money_laundering_gets_a_boost/; Int'l Bar Ass'n, *United States*, Anti-Money Laundering Forum (Mar. 5, 2012) https://www.anti-moneylaundering.org/northamerica/United_States_of_America.aspx.
151. Susan Beck, *Money Laundering Case Highlights ABA Stance on Lawyers' Obligations*, The Am. Law. (Aug. 1, 2016), http://www.americanlawyer.com/id=1202764081275/Money-Laundering-Case-Highlights-ABA-Stance-on-Lawyers-Obligations.
152. Voreacos, *supra* note 144.
153. *U.S. Fourth Mutual Evaluation*, *supra* note 52; *U.S. Third Mutual Evaluation*, *supra* note 51.
154. *U.S. Fourth Mutual Evaluation*, *supra* note 52, at 257–58.
155. Kevin Shepherd, Opinion, *ABA Needs a New Model Legal Ethics Rule*, Law360 (Apr. 6, 2017), https://www.law360.com/articles/910316/aba-needs-a-new-model-legal-ethics-rule.
156. Global Witness, Lowering the Bar: How American Lawyers Told Us How to Funnel Suspect Funds into the United States 1 (2016), https://www.globalwitness.org/documents/18208/Lowering_the_Bar.pdf.
157. *Id.*
158. *Id.*
159. *Id.*
160. *See, e.g.*, Eric Lipton & Julie Creswell, *Panama Papers*

Show How Rich United States Clients Hid Millions Abroad, The New York Times (June 5, 2016), https://www.nytimes.com/2016/06/06/us/panama-papers.html.

161. Beck, *supra* note 151.

162. *See, e.g.,* Jody Godoy, *Defense Bar Group No Fan of Shell Co. Transparency Bill*, Law360 (Oct. 2, 2017), https://www.law360.com/articles/957248/defense-bar-group-no-fan-of-shell-co-transparency-bill; Natalie Rodriguez, *Panama Papers Bring Law Firm Ethics Controversy to Fore*, Law360 (Apr. 6, 2016), https://www.law360.com/articles/780221/panama-papers-bring-law-firm-ethics-controversy-to-fore; Press Release, Sheldon Whitehouse, Senator, Following Panama Papers Release, Whitehouse Urges Action on the Incorporation Transparency and Law Enforcement Assistance Act (Apr. 27, 2016), https://www.whitehouse.senate.gov/news/release/following-panama-papers-release-whitehouse-urges-action-on-the-incorporation-transparency-and-law-enforcement-assistance-act.

163. S. 2489, 114th Cong. (2016); H.R. 4450, 114th Cong. (2016).

164. Press Release, Carolyn Maloney, Representative, Reps. Maloney, King and Senator Whitehouse Introduce Bills to Stop Anonymous Money Laundering Operations by Requiring Disclosure of Shell Corporation Beneficial Owners (Feb. 3, 2016), https://maloney.house.gov/media-center/press-releases/reps-maloney-king-and-senator-whitehouse-introduce-bills-to-stop; Press Release, Sheldon Whitehouse, Senator, Whitehouse Introduces Bill to Curb Money Laundering Through Shell Corporations (Feb. 3, 2016), https://www.whitehouse.senate.gov/news/release/whitehouse-introduces-bill-to-curb-money-laundering-through-shell-corporations.

165. S. 1454, 115th Cong. (2017).

166. Press Release, Sheldon Whitehouse, Senator, Whitehouse Introduces Bipartisan TITLE Act to Address Proliferation of Anonymous Shell Corporations in U.S. (June 28, 2017), https://www.whitehouse.senate.gov/news/release/whitehouse-introduces-bipartisan-title-act-to-address-proliferation-of-anonymous-shell-corporations-in-us.

167. H.R. 3089, 115th Cong. (2017).

168. Press Release, Carolyn Maloney, Representative, Reps. Maloney and King Join with Law Enforcement and Advocates to Call for End to Shell Company Secrecy (June 28, 2017), https://maloney.house.gov/media-center/press-releases/reps-maloney-and-king-join-with-law-enforcement-and-advocates-to-call.

169. S. 1717, 115th Cong. (2017); Press Release, U.S. Senate Committee on Finance, Wyden, Rubio Unveil Bill to Increase Transparency, Crack Down on Illicit Financial Crimes (Aug. 3, 2017), https://www.finance.senate.gov/ranking-members-news/wyden-rubio-unveil-bill-to-increase-transparency-crack-down-on-illicit-financial-crimes-.

170. S. 1717 § 3; S. 1454 § 3; H.R. 3089 § 3; S. 2489 § 3; H.R. 4450 § 3.

171. S. 1717 § 2; S. 1454 § 2; H.R. 3089 § 2; S. 2489 § 2; H.R. 4450 § 2.

172. S. 1717 § 3; S. 1454 § 3; H.R. 3089 § 3; S. 2489 § 3; H.R. 4450 § 3.

173. Stop Tax Haven Abuse Act, S. 851, 115th Cong. (2017); Stop Tax Haven Abuse Act, H.R. 1932, 115th Cong. (2017).

174. S. 1717 § 3; S. 1454 § 4; H.R. 3089 § 3; S. 851 § 206; H.R. 1932 § 206; S. 2489 § 4; H.R. 4450 § 3; *see also* Press Release, Sheldon Whitehouse, Senator, Whitehouse, Doggett Introduce Stop Tax Haven Abuse Act (Apr. 5, 2017) https://www.whitehouse.senate.gov/news/release/whitehouse-doggett-introduce-stop-tax-haven-abuse-act ("Currently, banks must abide by anti-money-laundering due diligence standards before taking on new customers. The bill would extend this commonsense requirement to professional[s] who help set up shell corporations").

175. Other AML legislation, which has been drafted and not yet introduced, such as the House Committee on Financial Services draft of the Counter Terrorism and Illicit Finance Act ("CTIFA"), does not include changing the definition of formation agents for purposes of the BSA. *See* Andrew N. D'Aversa & Peter D. Hardy, *Congress Proposes National Directory of Beneficial Owners of Legal Entities*, The Nat'l L. Rev. (Jan. 23, 2018), https://www.natlawreview.com/article/congress-proposes-national-directory-beneficial-owners-legal-entities; *see also* Letter from Hilarie Bass, Pres., Am. Bar Ass'n, to Reps. Jeb Hensarling and Maxine Waters (Nov. 27, 2017), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/gatekeeperregandtheprofessiontf(abalettertohfscfinalversionnov272017).authcheckdam.pdf [hereinafter Bass November 2017 Letter].

176. *See* Press Release, The White House, Fact Sheet: Obama Administration Announces Steps to Strengthen Financial Transparency, and Combat Money Laundering, Corruption, and Tax Evasion (May 5, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/05/05/fact-sheet-obama-administration-announces-steps-strengthen-financial; Press Release, U.S. Dep't of Treasury, Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion (May 5, 2016), https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx.

177. *Hearing on A Legislative Proposal on Counter Terrorism and Illicit Finance: Hearing Before the Senate Subcomm. on Fin. Inst. & Consumer Credit & Terrorism & Illicit Fin. of the S. Comm. on Fin. Serv.*, 115th Cong. 14 (2017) (prepared testimony of Stefanie Ostfeld, Deputy Head of U.S. Office, Global Witness).

178. *Id.* at 14–18.

179. *Hearing on Combating Money Laundering & Other Forms of Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. 3 (2018) (prepared testimony of Heather A. Lowe, Legal Counsel & Dir. of Gov't Affairs, Global Fin. Integrity).

180. *Hearing on Beneficial Ownership: Fighting Illicit International Financial Networks through Transparency Before S. Jud. Comm.*, 115th Cong. 1 (2018) (prepared statement of Sen. Charles Grassley).

181. *Id.* at 3.

182. *Id.*

183. *Hearing on Beneficial Ownership: Fighting Illicit International Financial Networks through Transparency Before S. Jud. Comm.*, 115th Cong. 1 (2018) (prepared testimony of Gary Kalman, Exec. Dir., Fin. Accountability & Transparency Coalition).

184. *Id.* at 10.

185. *Hearing* on *Beneficial Ownership: Fighting Illicit International Financial Networks through Transparency before S. Jud. Comm.*, 115th Cong. 19 (2018) (prepared testimony of Chip Poncy, Pres., Fin. Integrity Network).

186. *Id.*

187. *See, e.g.*, Letter from Hilarie Bass, Pres., Am. Bar Ass'n to Sens. Charles E. Grassley and Dianne Feinstein (Feb. 1, 2018), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/1feb2018-abalettertosjcopposings1454.authcheckdam.pdf [hereinafter Bass February 2018 Letter]; Press Release, Am. Bar Ass'n, ABA Opposes Legislation Imposing Beneficial Ownership Reporting on Small Businesses and Their Lawyers (Nov. 28, 2017), https://www.americanbar.org/news/abanews/aba-news-archives/2017/11/aba_opposes_legislat.html; Bass November 2017 Letter, *supra* note 176; Press Release, Am. Bar Ass'n, ABA Opposes Anti-Money Laundering Legislation that Erodes the Attorney-Client Privilege and Imposes Burdensome Regulations on Small Businesses, their Lawyers, and States (Oct. 2017), https://www.americanbar.org/

content/dam/aba/uncategorized/GAO/gatekeeperregandtheprofessiontf(abafactsheets1454s1717andhr3089october2017).authcheckdam.pdf; Press Release, Am. Bar Ass'n, ABA Opposes Anti-Money Laundering Legislation that Imposes Burdensome Regulations on Lawyers (June 2016), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/gatekeeperfactsheetjune2016.authcheckdam.pdf.

188. Letter from Paulette Brown, Pres., Am. Bar Ass'n, to Reps. Michael G. Fitzpatrick and Stephen F. Lynch (May 24, 2016), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2016may24_gatekeeperregandtheprofession.authcheckdam.pdf.
189. Shepherd, *supra* note 155.
190. Bass November 2017 Letter, *supra* note 175, at 1.
191. Bass February 2018 Letter, *supra* note 187, at 1.
192. *Id.* at 2.
193. *Id.* at 3.

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 served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia, tried 32 criminal trials, and briefed and argued criminal appeals. Ms. Brooker's practice focuses on internal investigations, regulatory enforcement, white-collar criminal defence, and compliance counseling. She represents financial institutions, multi-national companies, and individuals in connection with criminal, regulatory, and civil enforcement actions involving anti-money laundering (AML)/Bank Secrecy Act (BSA), sanctions, anti-corruption, securities, tax, and wire fraud.

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.

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.

Beneficial Ownership Transparency: A Critical Element of AML Compliance

Debevoise & Plimpton

Matthew L. Biben

For criminals trying to circumvent anti-money laundering and counter-terrorist financing measures, corporate vehicles – such as companies, trusts, foundations, and partnerships – are an attractive way to disguise illicit proceeds before introducing them into the financial system, further obscuring their origins and maximising the criminals' payment options.

Governments around the globe have concluded that this misuse of corporate vehicles could be significantly reduced if information regarding their beneficial owners was readily available to authorities, and many are amending their incorporation processes to capture and document this information. In the United States, however, the incorporation process takes place at the state level under the direction of each individual Secretary of State. The state Secretaries of State are opposed to legislation that would require them to collect beneficial owner information, claiming that such requirements present an unnecessary administrative burden.

This article discusses the evolution of the mandate for governments to establish and maintain reliable corporate registries and examines the particular forces complicating this issue in the United States.

The Misuse of Corporate Entities

In the United States, the notion that a corporation has a legal personality distinct from the natural persons who comprise it reaches back to the early days of U.S. constitutional law. As defined by the United States Supreme Court in a case involving Dartmouth College, whose corporate charter was granted by the British crown in 1769, a corporation is "an artificial being, invisible, intangible, and existing only in contemplation of law."[1]

However, without laws requiring disclosure of its owners, the "invisible, intangible" nature of a corporation can easily be used by bad actors to maintain their anonymity while enjoying the proceeds of their crimes. News events provide a steady stream of colourful examples. For example, Victor Bout, a Russian arms dealer who was convicted in 2011 of conspiring to sell millions of dollars of weapons to the Revolutionary Armed Forces of Colombia, used at least 12 companies incorporated in Texas, Florida, and Delaware to carry out his activities.

In 2016, the release of the so-called Panama Papers, leaked from the Panamanian law firm of Mossack Fonseca, disclosed the extensive use of shell companies to hide beneficial ownership interests in bank accounts. According to the International Consortium of Investigative Journalists, the network of investigative journalists and media organisations that published the documents, the Panama Papers included files on 140 politicians from more than 50 countries who were connected to offshore companies in 21 tax havens.[2] While the use of shell companies is not unlawful, the way in which they were used, as documented in the Panama Papers, led to significant political disruption: the disclosures are thought to have contributed to the 2016 resignation of the Prime Minister of Iceland and the 2017 indictment of Pakistan Prime Minister Nawaz Sharif, as well as numerous corruption and tax fraud investigations worldwide.[3]

The Risk for Financial Institutions

Historically, governments have delegated much of the responsibility for policing money laundering activity to financial institutions, arguing that they are better suited for the task. However, corporate accounts pose unique compliance challenges not just for the financial institutions opening and maintaining these accounts, but also for firms acting as intermediaries, particularly correspondent banks processing wire transfers to or from these accounts. When these transactions trigger automated alerts based on their unusual size or frequency, ascertaining the purpose of the transactions is often difficult if not impossible. The explanations provided to the correspondent banks by their customers – that is, the banks initiating or receiving the transfers – frequently fail to satisfy the concerns of internal compliance officers. If these concerns remain unresolved, the bank acting as intermediary often must file one or more suspicious activity reports or risk facing substantial fines from regulators for a failure to maintain an effective AML compliance programme. Such fines exceeded $2 billion globally in 2017.[4]

A Global Consensus with Diverse Solutions

In recent years, however, a global consensus has emerged that transparency of beneficial ownership is a powerful means of reducing the misuse of corporate vehicles. In 2012, the Financial Action Task Force ("FATF"), the primary inter-governmental body that sets standards for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system, issued revised standards on corporate beneficial ownership.[5] In 2013, the G-8 countries[6] endorsed core principles on beneficial ownership consistent with the FATF standards and published action plans setting out the steps they will take to enhance transparency. In 2014, FATF issued additional guidance[7] and the G-20 countries adopted a high-level policy on beneficial ownership transparency.[8]

In May 2015, the European Union ("EU") enacted the Fourth Anti-Money Laundering Directive, setting goals for its 28 member countries. The Fourth Directive introduced measures to provide enhanced clarity and accessibility of Ultimate Beneficial Owner ("UBO") information for companies by requiring companies to

hold information about their beneficial ownership and to make this information available to third parties via a public register. European states had until June 26, 2017 to enact the changes put forth in the Directive, and they are currently in varying stages of compliance and implementation.

In July 2017, the United States Library of Congress ("LOC") issued a report which surveyed the laws related to registration of beneficial owners and disclosure of information on corporate data in jurisdictions representing all major geographic regions of the world.[9] Most of the countries in the survey had recently amended their legislation (e.g., Argentina, Brazil, Costa Rica, France, Germany, Italy, Jamaica, Jordan, Pakistan, Singapore, South Africa, Sweden, United Kingdom) or were working on amending their laws (Afghanistan, India, Netherlands). Among the G-7 countries,[10] only Canada and Japan had not changed their national laws, even though both countries had committed to meeting FATF requirements. At the time, Canada reported that it did not "require that the beneficial ownership and company formation of all legal persons organised for profit be reported".[11] Japan also did not have a law that requires companies to disclose their beneficial ownership, but a new rule providing for disclosure of major shareholders was reportedly adopted in 2016.[12]

The countries surveyed that address corporate beneficial ownership do so through a variety of legal mechanisms, including corporate laws, registration rules, regulations implementing EU directives, and anti-money laundering legislation.[13] They require companies to report information on beneficial owners to the registering authorities, which are usually state or local governments. In some unitary states, this function is performed by a designated national institution. According to the survey, corporate beneficial owner information is collected by business registrars (Afghanistan, Argentina, India, Sweden, United Kingdom), national tax authorities (Brazil), securities regulators (Australia, Pakistan), a securities exchange (South Africa), central banks (Armenia, Costa Rica), local courts (France) and, in the EU, by a designated central registry in each Member State.

One major difference among the countries surveyed was in the definition of "beneficial owner".[14] The EU and its Member States follow FATF guidance, which defines a beneficial owner as a "natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted". Other countries add to the definition individuals with a "relevant interest" (Australia) or a "person with significant control" (United Kingdom), as determined by percentages of shares owned and the total number of shareholders. Some countries, such as Israel and Spain, exempt from reporting requirements individuals who own less than a particular percentage of company's shares; other countries exempt specific groups of individuals or companies working in select business sectors.

Access to the corporate data reported in registration documents is determined differently in each country.[15] At the time of the survey, some jurisdictions had created or were working on establishing open access to public registers of beneficial ownership (Afghanistan, Argentina, Australia, France, Israel, Jamaica, Netherlands, United Kingdom), although some may require the payment of fees (Australia, Jamaica, Netherlands). The EU Member States and Japan provide access to government institutions, obliged entities, and all who may have "legitimate interests" without defining the parameters of these interests. Others limit access to law enforcement (Singapore), monitoring government authorities (Armenia, Brazil, Costa Rica, Mexico), or members of the company (India).

The Scope of the Problem in the United States

In the United States, corporations are exclusively creations of state law, with each of the 50 states retaining control of the incorporation process in their respective jurisdictions through the offices of their Secretaries of State. However, few states have made collecting beneficial owner information a priority. Findings in recent federal legislation summarise the consequences of this arrangement:[16]

- Nearly 2,000,000 corporations and limited liability companies are being formed under the laws of the states each year.
- Very few states obtain meaningful information about the beneficial owners of the corporations and limited liability companies formed under their laws. Indeed, a person forming a corporation or limited liability company within the United States typically provides less information to the state of incorporation than is needed to obtain a bank account or driver's licence.
- Terrorists and other criminals have exploited the weaknesses in state formation procedures to conceal their identities when forming corporations or limited liability companies in the United States.
- Many states have established automated procedures that allow a person to form a new corporation or limited liability company within 24 hours of filing an online application, without any prior review of the application by a state official.
- Dozens of internet websites promote states with particularly lax beneficial ownership transparency requirements as attractive locations for the formation of new corporations, essentially inviting terrorists and other wrongdoers to form entities within the United States.

Not surprisingly, FATF has called the United States framework "seriously deficient" and has urged the United States to take corrective action.[17] Federal officials have long urged the states to develop their own solutions to effectively reform their corporate formation practices. Unfortunately, solutions proposed by the states through the National Association of Secretaries of State ("NASS") have failed to address fundamental issues. For example, a NASS proposal issued in 2007 did not require states to obtain the names of the natural individuals who would be the beneficial owners of a U.S. corporation or LLC; instead, states could obtain a list of a company's "owners of record" who can be, and often are, offshore corporations or trusts.[18] The NASS proposal also did not require the states to maintain the beneficial ownership information themselves, or to supply it to law enforcement in response to a subpoena or summons.[19]

Why have the individual states not taken a more aggressive stance on beneficial ownership? A 2008 statement by Senator Carl Levin introducing legislation that would create a nationwide transparency framework called on the states to "recognize the homeland security problem they've created".[20] Senator Levin went on to identify two sets of forces preventing them from doing so:[21]

Part of the difficulty is that the States have a wide range of practices, which differ on the extent to which they rely on incorporation fees as a major source of revenue, and differ on the extent to which they attract non-U.S. persons as incorporators. In addition, the States are competing against each other to attract persons who want to set up U.S. corporations, and that competition creates pressure for each individual State to favour procedures that allow quick and easy incorporations. It's a classic case of competition causing a race to the bottom, making it difficult for any one State to do the right thing and request the names of the beneficial owners.

Current U.S. Proposals

In May 2016, FinCEN expanded its customer due diligence ("CDD") rule by requiring financial institutions to establish procedures to identify the beneficial owners of legal entity customers when a new account is opened. FATF pointed out, however, that this move failed to require the disclosure of beneficial owners at the time that legal entities are formed and rated the United States with the lowest possible score in its efforts to prevent criminals from using legal entities to hide and move money.[22]

On June 28, 2017, the True Incorporation Transparency for Law Enforcement Act ("TITLE Act") was introduced in the Senate with bipartisan support.[23] Under the TITLE Act and subject to certain exemptions, each applicant to form a new corporation or limited liability company under the laws of a state would be required to provide to the state information on the beneficial owners of the corporation or limited liability company. The term "beneficial owner" is defined as each natural person who, directly or indirectly: (i) exercises substantial control over a corporation or limited liability company through ownership interests, voting rights, agreement, or otherwise; or (ii) has a substantial interest in or receives substantial economic benefits from the assets of a corporation or the assets of a limited liability company.

Under this bill, it would be up to each state to decide whether to make beneficial ownership information publicly available. However, disclosure would be required in response to:

- a subpoena from a local, State, or Federal agency or a congressional committee or subcommittee;
- a written request from FinCEN or a Federal agency on behalf of another country; or
- a written request made by a financial institution, with the consent of the customer, for purposes of compliance by the financial institution with CDD requirements.

The bill includes provisions for corporate formation agents licensed by the states and adds those businesses to the list of entities required to establish anti-money laundering programmes.

The state Secretaries of State, through NASS, have said they oppose this bill as well as any other proposal that would require them to collect beneficial ownership information – a position they have held since 2008.[24] NASS claims the TITLE Act is unnecessary because it would require states to collect information that is already being collected by the federal government in various forms and processes,[25] or will soon be collected by financial institutions pursuant to FinCEN's new CDD rule. However, none of these alternatives – either alone or in combination – would satisfy the global standard set by FATF that requires the disclosure of beneficial owners at the time that legal entities are formed.

Two other bipartisan bills introduced in 2017 attempt to address what seems to be the states' primary objection – the burden of expanding their incorporation processes. Both bills, one in the House of Representatives (HR. 3089),[26] and one in the Senate (S.1717),[27] are titled the "Corporate Transparency Act of 2017". Under these bills, if a state does not have a system of incorporation that collects the requisite beneficial ownership information, FinCEN would bear the burden of collecting and managing the additional information. However, in December 2017, NASS issued a statement in opposition to both HR. 3089 and S.1717.[28]

Financial institutions support such legislation but stress the importance of being able to obtain access to reported beneficial ownership information. They note, appropriately, that under the current AML regime, many if not most of the resources devoted to identifying money laundering and terrorist financing are provided by financial institutions, and that denying them access to this important information would significantly undermine the goals of any bill.[29]

Conclusion

The United States is one of many nations that has concluded that the misuse of corporate vehicles could be significantly reduced if beneficial owner information was collected at the time of corporate formation and was made available to authorities. While the U.S. has imposed a new CDD rule requiring financial institutions to establish procedures to identify the beneficial owners of legal entity customers, there is recognition that more must be done. In the absence of collective action by the states, the U.S. federal government has appropriately stepped in to legislate a solution, but with no success thus far.

While many elements of anti-money laundering responsibilities fall to financial institutions, beneficial ownership is a distinct component of corporate formation – and thus responsibility for its transparency should fall to the government, which, in the United States, means the individual states.

To put things in perspective, it is helpful to recall a similar issue years ago involving Nauru, a small island nation in Micronesia. After allowing its primary natural resource, phosphate, to be depleted through strip mining, the island resorted to selling offshore banking licences. Four hundred banks listed the same 1,000 square foot wooden shack as their headquarters though none had a physical presence in Nauru or, for that matter, in any other country. The resulting banking activity did not have any adverse impacts on Nauru, but it did create significant risk to the global financial system, leading FATF to place Nauru on the Non-Cooperative Countries and Territories' list in June 2000, and FinCEN to designate Nauru as a country of primary money laundering concern in 2002.[30] When considering their corporate formation policies, jurisdictions would be well advised to weigh the global effects of local actions – particularly when those actions affect money laundering enforcement efforts across nations.

Endnotes

1. Trustees of *Dartmouth College v. Woodward*, 17 U.S. (4 Wheat.) 518, 636 (1819).
2. *See*, International Consortium of Investigative Journalists, Panama Papers, www.icij.org/investigations/panama-papers/.
3. *Id*.
4. *See, e.g.*, Debevoise & Plimpton LLP, 2017 Anti-Money Laundering Year in Review (Feb. 2, 2018), *www.debevoise.com/insights/publications/2018/02/2017-anti-money-laundering-year-in-review*.
5. FATF, Int'l Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012) (updated Feb. 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
6. At the time, the G-8 countries were Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and Russia. In 2014, Russia was suspended following the annexation of Crimea, whereupon the group's name reverted to the G-7.
7. FATF, Transparency and Beneficial Ownership (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.
8. The G-20, or Group of Twenty, is comprised of Argentina, Australia, Brazil, Canada, China, European Union, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom and the United States.

9. United States Library of Congress, Disclosure of Beneficial Ownership in Selected Countries (July 2017), https://www.loc.gov/law/help/beneficial-ownership/chart.php [hereinafter LOC Survey].
10. At the time, the G-7 countries were Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.
11. LOC Survey at 1.
12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. True Incorporation Transparency for Law Enforcement Act, S. 1454, 115th Cong. (2017) [hereinafter *S. 1454*].
17. FATF, Mutual Evaluation Report, Anti-money laundering and counter-terrorist financing measures of the United States (December 2016) [hereinafter *FATF 2016 U.S. Mutual Evaluation*].
18. Congressional Record, *Introducing the Incorporation Transparency and Law Enforcement Assistance Act*, 110th Cong., Vol. 154, Pt. 6, at 7621 (May 1, 2008) (statement of Sen. Carl Levin, S. Comm. on Homeland Sec. and Gov't Affairs), https://www.gpo.gov/fdsys/pkg/CRECB-2008-pt6/pdf/CRECB-2008-pt6-Pg7617.pdf [hereinafter *Senator Levin Statement*].
19. *Id*.
20. *Id*.
21. *Id*.
22. FATF 2016 U.S. Mutual Evaluation.
23. S.1454.
24. See National Association of Secretaries of State (NASS) website at www.nass.org/initiatives/state-incorporation-collection-company-ownership-info [hereinafter *NASS Website*].
25. See NASS Website. The federal forms and processes referenced by NASS are the Internal Revenue Service's (IRS) Revised Form SS-4, which requires certain disclosures when applying for an Employer Identification Number (EIN), and the U.S. Treasury Department's Report of Foreign Bank and Financial Accounts Report (FBAR), which must be filed yearly by U.S. persons with a financial interest in or signature authority over financial accounts located outside of the U.S., subject to a minimum threshold. FATF has specifically outlined why the EIN mechanism does not satisfy the requisite beneficial ownership standard. FATF 2016 U.S. Mutual Evaluation, at 154, 158, 224–226.
26. Corporate Transparency Act of 2017, H.R. 3089, 115th Cong. (2017).
27. Corporate Transparency Act of 2017, S. 1717, 115th Cong. (2017).
28. Chris Marquette, *Congress Targets Shell Company Laws that Lure Global Criminals to US*, Congressional Quarterly Inc., 2017 WL 6379121(December 14, 2017) [quoting a statement from the executive director of the NASS].
29. The Clearing House, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement (February 2017).
30. See FinCEN, Imposition of Special Measures Against the Country of Nauru (April 17, 2003), https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/imposition-special-measures-against-country.

Acknowledgments

The author would like to acknowledge the assistance of Kevin J. Suttlehan in the preparation of this chapter. Kevin is an anti-money laundering expert focused on regulatory and enforcement matters with an emphasis on internal investigations and financial crime compliance issues. The author would also like to acknowledge the assistance of Zila R. Acosta-Grimes in the preparation of this chapter. Zila is a member of the firm's Financial Institutions Group based in the New York office.

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

Tel: +1 212 909 6000
Email: mbiben@debevoise.com
URL: www.debevoise.com

Matthew L. Biben is a litigation partner, co-leader of the firm's Banking Industry Group, and member of the firm's White Collar & Regulatory Defense Group. His practice is focused on the expert negotiations and litigation of complex and diverse regulatory and enforcement matters on behalf of both individuals and organisations, with a concentration on matters related to financial institutions and complex situations involving the government. Mr. Biben has garnered extensive experience advising boards and senior management through extensive enforcement and advisory work. He routinely acts as counsel in internal investigations of both domestic and international matters involving the DOJ, SEC, FRB, OCC, CFPR, NYDFS, State Attorneys General and foreign regulators. He is recommended by *The Legal 500 US* (2016) where he is described as a "tenacious but balanced litigator".

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.

We assist clients in:

- reviewing, revising and implementing anti-money laundering and sanctions-related compliance policies and procedures;
- performing compliance assessments;
- providing anti-money laundering and sanctions training;
- leading internal investigations regarding potential compliance issues;
- responding to regulatory and law-enforcement inquiries regarding anti-money laundering and sanctions; and
- defending proceedings and enforcement actions instituted by the U.S. Justice Department, U.S. federal banking regulators, OFAC, the UK Serious & Organised Crime Agency and the New York Department of Financial Services.

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

Daniel Holman

Barbara Stettner

Allen & Overy LLP

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 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 as: (1) "a medium of exchange"; a (2) "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 time stamped 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 to 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

Despite calls for the adoption of global AML standards for cryptocurrency trading,[22] no such uniform rules have yet emerged. There has nonetheless been some convergence toward the FATF 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 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] 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.

European Union Regulatory Approach

The most recent European-level AML directive, the Fourth Money Laundering Directive ("**MLD4**"),[64] did not explicitly address cryptocurrency, and the European Commission has not interpreted its existing regulatory guidance to require extension of the MLD4 regime to cryptocurrencies.[65] As part of the development of the proposed Fifth Money Laundering Directive ("**MLD5**"),[66] however, the European Parliament and European Council reached an agreement in December 2017 that would extend AML obligations to firms operating centralised cryptocurrency exchanges or custodial wallet providers[67] for cryptocurrencies[68] by adding them to the definition of "obliged entities" contained in the existing directives.[69] These amendments would require EU Member States to subject those service providers to the same obligations as banks and other financial institutions under MLD4 – including CIP and beneficial ownership identification, KYC, transaction monitoring, and suspicious activity reporting – and will subject those providers to supervision by the competent national authorities for these areas.

Once MLD5 is published, Member States will have 18 months to implement most provisions into national law.[70] With publication of MLD5 anticipated to occur in mid-2018, national implementation of these requirements may be expected by late 2019 or early 2020.

While MLD5 is pending, some EU jurisdictions have 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[71] in compliance with MLD4 in 2017 (which was done via a legislative decree, "**AML4 Decree**"),[72] it simultaneously incorporated definitions for cryptocurrency consistent with the FATF-definition[73] and classified cryptocurrency service providers[74] that provide cryptocurrency-to-fiat conversion services as "non-financial intermediaries" regulated under the AML Decree.[75] Such service providers are consequently subject to Italian AML obligations,[76] including KYC,[77] record keeping and communications to the authorities,[78] suspicious transaction reporting,[79] and, as a consequence of the pseudo-anonymity of blockchain users, enhanced due diligence ("**EDD**").[80] 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[81] 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).[82] 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.[83]

Although Italy's investment services authority, CONSOB,[84] 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.[85] A 2015 Bank of Italy communication[86] 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.[87] 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.

(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**").[88] 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.[89] 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"[90] under the German Money Laundering Act ("**GWG**"),[91] transposing the MLD4 AML requirements.[92] 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.[93] 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 have not formally extended their AML regulation to cover cryptocurrency activities.

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**")[94] has provided assurance that VCE and wallet services for currency-like cryptocurrencies fall outside the scope of the DFSA[95] and, consequently, are in general not covered "institutions" for purposes of the Act for the Prevention of Money Laundering and Financing of Terrorism ("**Wwft**").[96] When MLD5 is implemented, however, the Wwft will extend to these entities as discussed above.[97] The Minister of Finance expects to complete the implementation of this amendment by the end of 2019.[98]

Although a lower court ruled in 2014 that Bitcoins do not themselves qualify as "common money",[99] as a practical matter many Dutch banks and other financial institutions have been reluctant to accept proceeds that derive from cryptocurrency exchange transactions if they cannot validate the origin of these funds. Additionally, cryptocurrencies that have the character of stocks or bonds would arguably also qualify as "securities" and therefore as "financial instruments" under the DFSA,[100] such that a provider of such a cryptocurrency or of investment services for such a cryptocurrency would be subject to the DFSA and, insofar as it relates to investment services, the Wwft.[101] However, to date there has been no formal action reaching such a conclusion.

(d) UK

In the UK, the prevailing view of regulators has been to treat cryptocurrencies as a commodity, rather than a currency or a security. On this basis, the UK Financial Conduct Authority ("**FCA**") chief executive Andrew Bailey recently confirmed 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.[102] The FCA has also confirmed that,[103] in its view, cryptocurrencies such as Bitcoin are not "specified investments" for the purposes of the Financial Services and Markets Act ("**FSMA**") 2000 (Regulated Activities) Order 2001.[104] Nonetheless, given the breadth of products that may be labelled as cryptocurrencies, there is a risk that some coins or tokens (including those issued as part of an ICO) may constitute transferable securities and fall within the prospectus regime under the FSMA 2000, or alternatively, depending upon how they are structured, some ICOs may instead amount to a collective investment scheme under section 235 of the FSMA. Derivatives that reference a cryptocurrency are also capable of being regulated investments.[105]

Unless one of the regulated financial services regimes above is triggered, cryptocurrency activities are unlikely to currently fall within the scope of the UK Money Laundering Regulations 2017.[106] Changes currently proposed at the EU level (and supported by the UK Treasury) would result in cryptocurrency exchanges and custodian wallet providers' activities being within the scope of AML laws. Subject to Brexit, the UK will need to implement these provisions into national law and regulation within 18 months, meaning such amendments may apply by late 2019, if not sooner. Even if Brexit relieves the UK of these obligations before the MLD5 implementation deadline,[107] UK regulators or legislators may choose to design a bespoke regime to regulate and govern cryptocurrencies and their exchange, or to otherwise broaden existing financial services regulatory regimes to cover cryptocurrency activities.

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 constitute a predicate crime for certain money laundering offences under the Proceeds of Crime Act 2002.

Separate and apart from whether dealings with cryptocurrencies may implicate FI status under UK law, cryptocurrencies or the proceeds of their sale that could be the subject of a restraint order or confiscation order to the extent that they constitute criminal property under the Proceeds of Crime Act 2002 ("**POCA**"), and concealing or handling such criminal property could trigger the money laundering offences under POCA.[108] Moreover, where firms operate within the regulatory perimeter in breach of the FSMA general prohibition (e.g., by issuing security tokens without requisite FCA authorisation), such a breach would constitute a criminal offence, and thereby constitute a predicate crime for the primary money laundering offences under 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 crypto businesses, while Korea has yet to settle on a regulatory scheme of any kind.

(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.[109]

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.[110]

- 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.

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[111] and to create a registration requirement for "Virtual Currency Exchange Operators" ("**VCEOs**").[112] VCEO licences permit holders to engage in the exchange, purchase, sale, and safekeeping of cryptocurrencies on behalf of third parties, and to engage in ICOs subject to pre-approval by the FSA. 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.[113] Since licences were first issued to VCEOs on September 30, 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.[114]

(c) Korea

As at the time of writing, South Korea continues deliberations on reaching a comprehensive cryptocurrency regulatory scheme, resulting in a situation that some commentators have described as "a state of 'deliberate ambiguity'".[115] After initially legalising Bitcoin service providers for payments, transfers, and trades in July 2017,[116] cybersecurity and AML concerns led to the issuance of a ban on ICOs in September 2017.[117] Though subsequent remarks by public officials even suggested shutting down exchanges entirely, reports suggest that the ban has not been strictly enforced while the government's internal consultations continue[118] and that limitations will be lifted once a formal legal framework can be established.[119]

Because of the legal uncertainty regarding the future status of cryptocurrencies, the Korean Financial Services Commission ("**FSC**") has begun to regulate cryptocurrencies through its authority to regulate banks pursuant to its existing statutory powers. These measures, announced in January 2018, require cryptocurrency trading to occur through real-name bank accounts linked to cryptocurrency exchanges.[120] The FSC also introduced a mandatory "guideline" with respect to cryptocurrency-linked accounts to ensure bank compliance with AML.[121] Among other things, the guideline requires banks to "conduct [EDD] in transaction[s] with cryptocurrency exchanges to make sure users' money [is] in safe hands. The EDD requires banks to verify additional information for cryptocurrency exchanges: the purpose of financial transactions and the source of money; details about services that the exchanges provide; whether the exchanges are using real-name accounts; and whether the exchanges verify their users' identification".[122] The guideline also mandates banks to "refuse to offer accounts to cryptocurrency exchanges if they do not provide their users' ID information".[123]

(d) 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.[124] 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.[125] 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.[126]

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 FIs subject to AML requirements to stay abreast of new criminal uses.

- **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.[127]

- **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.
- **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.
- **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.

- **Placement**: The ability to rapidly and anonymously open anonymous accounts provides a low-risk means for criminal groups to convert and consolidate illicit cash.
- **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.[128] 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.[129] 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.
- **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.[130] 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.
- **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.[131] 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.[132]

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.[133]

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 fulfilment 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"[134] 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[135] and detection of structuring payments.[136] 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.[137] 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.[138] 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.[139] 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".[140]

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:

- **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?
- **Monitoring and reporting**: Does the customer have mechanisms in place for account monitoring and procedures in place for required reporting?
- **Geographic controls**: Is the service able to control the jurisdictions in which its services are accessed?
- **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.[141]

(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.[142] 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.

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/documents/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. See FATF 2015 Guidance, *supra* note 2, at 12.
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) cheque casher; (3) issuer of traveller's cheques, money orders, or stored value; (4) seller or redeemer of traveller's 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 dealer 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. 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].
65. *Id.* Specifically, the European Parliament and the Council of the European Union determined that the rules and regulation of the MLD4 do 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].
66. Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849, *supra* note 66.
67. *I.e.*, wallets that hold the customer's private keys, and therefore have effective custody of the customer's blockchain account.
68. The proposal for MLD5 contains the following definition of virtual currencies: "'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849, *supra* note 66.
69. EU Directive 2015/849, *supra* note 65.
70. More time may be permitted for provisions which have different transposition deadlines.
71. Legislative Decree n. 231/2007 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Nov. 21, 2007) (It.).
72. Legislative Decree n. 90/2017 (EU MLD4) (May 25, 2017) (entry into force of the new AML Decree on July 4, 2017) [hereinafter AML4 Decree] (It.).
73. 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).
74. 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*).
75. *Id.* art. 3 ¶ 5(i).
76. *Id.* art. 3.
77. *Id.* arts. 17–30.
78. *Id.* arts. 31–34.
79. *Id.* arts. 35–41.
80. 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.
81. Held by the Italian Organization of Agents and Mediators.
82. AML4 Decree, *supra* note 73, at art. 8 (by amending Legislative Decree n.141 of Aug. 13, 2010 art. 17-*bis*.).
83. 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.).
84. *Commissione Nazionale per le Società e la Borsa*.
85. Legislative Decree n. 58 of Feb. 24, 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.
86. *Banca D'Italia Eurosistem*, *Avvertenza sull'utilizzo delle cosiddette* "*valute virtuali*", Jan. 30, 2015 (It.).
87. *See* Legislative Decree n. 385 of Sept. 1, 1993 arts. 130–131, 131-*ter*, 166 (It.).
88. 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.).
89. Likewise, the creation of new cryptocurrency by solving complex mathematical computational tasks (mining) does not constitute a regulated activity according to the KWG.

90. "*Verpflichtete*".
91. *Geldwäschegesetz* [GwG] [Money Laundering Act], Aug. 13, 2008 at §§ 2(1)(1)-(2) (Ger.).
92. *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.).
93. 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.).
94. *Beantwoording schriftelijke Kamervragen Nijboer over het gebruik van en toezicht op nieuwe digitale betaalmiddelen zoals de Bitcoin*, FM/2013/1939 U (19 Dec. 2013) [hereinafter FM/2013/1939 U] (Neth.).
95. *Id.*
96. *Wet ter voorkoming van witwassen en financiering van* terrorisme Aug. 1, 2008, art. 1, ¶ 1, sub a (Neth.) [hereinafter Wwft].
97. *I.e.*, VCEs and wallet providers offering custodial services of credentials necessary to access virtual currencies.
98. Chairman of the House of Representatives of the States General, *Letter on Cryptocurrency Developments* (8 Mar. 2018), 2018-0000033278, https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/08/achtergrond-en-overige-informatie-over-cryptovaluta (Neth.).
99. Court of Overijssel 14 May 2014, ECLI:NL:RBOVE:2014:2667.
100. "*Effect*", as defined in article 1:1 of the DFSA. FM/2013/1939 U, *supra* note 95, art. 1:1. Specifically, such securities would potentially be a "*financieel instrument*", as defined in article 1:1 of the DFSA). *Id.*
101. Wwft, *supra* note 97, art. 1, ¶ 1, sub a.
102. Andrew Baily, BBC's Newsnight (Dec. 14, 2017).
103. Letter from Andrew Bailey, FCA, to Nicky Morgan, MP, Treasury Select Committee (dated Jan. 30, 2018).
104. Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (UK).
105. To date, the status of cryptocurrencies 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, for so 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.
106. *I.e.*, the UK implementation of the MLD4.
107. The UK government recently established a crypto-assets taskforce, consisting of the UK Treasury, the Bank of England, and the UK Financial Conduct Authority, to study the issue and make legislative proposals.
108. Proceeds of Crime Act 2002 §§ 327–329 (UK).
109. High People's Court of Heilongjiang Province of China (2016), http://wenshu.court.gov.cn/Content/Content?DocID=ce26a599-64e9-44ab-96fd-b04617d482b4 (China).
110. 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).
111. 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).
112. *See* art. 63-5 of the Amended Payment Services Act (Japan).
113. Law No. 22 of 2007. The PTCP was amended in April 2017 to include VCEOs in this definition.
114. *More Japanese Cryptocurrency Exchanges to Close*, Nikkei (Mar. 29, 2018), https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close.
115. Andrew Salmon, *Korean Cryptocurrency Market Faces New Regulatory Risk*, Asia Times (Mar. 19, 2018), http://www.atimes.com/article/korean-cryptocurrency-market-faces-new-regulatory-risk/ (quoting Ahn Chan-sik, who leads the Technology and Communications practice at Hwang, Mok, Park).
116. Son Ji-hyoung, *Bills Move to Give Bitcoin Legal Grounds*, Korea Herald (July 3, 2017), http://www.koreaherald.com/view.php?ud=20170703000867.
117. Forbes Tech. Council, *How Will The China And South Korea ICO Bans Impact Cryptocurrencies?*, Forbes (Dec. 11, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/11/how-will-the-china-and-south-korea-ico-bans-impact-cryptocurrencies/#44fe17ef5124.
118. Dahee Kim & Ju-min Park, *South Korea Keeps Investors Guessing on Cryptocurrency Regulation*, Reuters (Feb. 28, 2018), https://www.reuters.com/article/us-malaysia-cenbank-cybersecurity-incide/malaysian-central-bank-says-foiled-attempted-cyber-heist-idUSKBN1H50YF (citing government statements that further consultations are needed before the government will reach a final conclusion as to how to regulate the sector).
119. Eli Meixler, *It Looks Like South Korea is Planning to Allow ICOs and Regulate Crypto Trading After All*, Fortune (Mar. 13, 2018), http://fortune.com/2018/03/12/south-korea-cryptocurrency-ico/.
120. Press Release, South Korean Fin. Servs. Comm'n, Financial Measures to Curb Speculation in Cryptocurrency Trading (Jan. 23, 2018), http://www.fsc.go.kr/downManager?bbsid=BBS0048&no=123388 (S. Kor.).
121. *Id.*
122. *Id.*
123. *Id.*
124. Australian Secs. & Inv. Comm'n, Information Sheet 225 (Sept. 2017), http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#shares (Austl.).
125. 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.

126. 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).
127. *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.
128. 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.
129. Europol, Press Release, Illegal Network Used Cryptocurrencies and Credit 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.
130. *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.).
131. 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.
132. *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.
133. 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.
134. *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.
135. 31 C.F.R. § 1010.313.
136. 31 U.S.C. § 5324.
137. 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.
138. *Id*. at 3 (stating that "it is reasonable and appropriate for a banking organization to insist that a money services business provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements").
139. 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).
140. *Id*.
141. 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.
142. FATF-modelled AML regimes include prohibitions on the acceptance of proceeds of a crime ("illicit proceeds"). *See*, *e.g.*, 18 U.S.C. §§ 1956–57.

Acknowledgment

The authors wish to thank the following attorneys for their significant contributions to this chapter: Jane Jiang, Tiantian Wang and Jason Song (China); Dennis Kunschke (Germany); Giovanni Battista Donato, Emanuela Semino and Amilcare Sada (Italy); Neyah van der Aa, Robin van Duijnhoven and Daphne van der Houwen (the Netherlands); Ben Regnard-Weinrabe and Heenal Vasu (UK); and Sam Brown, Bill Satchell, Justin Cooke, Lindsay Kennedy, Derek Manners, and Chelsea Pizzola (U.S.).

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

Tel: +1 202 683 3853
Email: daniel.holman@allenovery.com
URL: www.allenovery.com

Daniel is an associate in the Investigations and Litigation practice group in the firm's Washington, D.C. office. His practice includes supporting clients in the conduct of multijurisdictional internal investigations and advocating for them in contentious regulatory proceedings in the areas of competition, anticorruption, anti-money laundering, government procurement, pay-to-play, campaign finance, and lobbying regulation. Daniel also advises clients on compliance obligations in these areas. Prior to joining Allen & Overy, Daniel was a Visiting Fellow at the UNAM Legal Research Institute in Mexico City.

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.

Through a Mirror, Darkly: AML Risk in Trade Finance

Alma Angotti

Robert Dedman

Navigant Consulting

Introduction

International trade is the lifeblood of the world economy. However, financing – or passing through funds from – international trade transactions places financial institutions at significant risk of being used as conduits for a variety of financial crime, including trade based money laundering (TBML), terrorist financing and certain forms of predicate criminality. And the financial value of such illicit flows of funds is potentially significant: Global Financial Integrity (GFI) estimated in a report published in April 2017[1] that in developing and emerging economies illicit inflows and outflows accounted for between 14 and 24% of their total trade in the years between 2005 and 2014. To give an idea of scale, the GFI report estimates that, in dollar terms, illicit inflows and outflows accounted for between US$620bn and US$970bn in 2014 alone.

Criminals exploit a number of factors to make use of the trade finance process for their illicit activities, including:

- the fact that the importer and exporter may be geographically distant from one another, and the importer may not even see the goods until they arrive at their port of destination;
- the fact that the underlying goods for which trade finance may traverse significant distances – most often by ship – and cross multiple borders; and
- the sheer volume of international trade makes it relatively straightforward to hide illicit transactions in plain sight.

While regulators and international standard setting bodies have – for more than a decade – published information for firms about how to identify and prevent TBML, regulatory action against financial institutions for TBML failings has been relatively rare. Despite the scarcity of significant enforcement action, regulators have set clear expectations of the industry, and when they have focused on the industry's approach to trade finance, they have found significant shortcomings in how financial institutions deal with TBML risk. As such, a strong compliance programme which aims to detect and prevent potential TBML is vital for any firm engaged in trade finance activity.

The different types of trade finance transaction also pose different levels of risk to financial institutions, and bring with them different challenges in terms of institutions' ability to detect illicit activity.

Documentary trade finance transactions[2] (which account for approximately 20% of all transactions) involve a bank issuing documents on behalf of a customer guaranteeing payment if certain specified terms are met[3]. Once the payment has been made, the goods are then released to the buyer. The financial institution concerned would therefore usually have access to the key documents evidencing the transaction, including a description of the goods themselves, details of their origin and destination (and sometimes the vessel on which they have been shipped), and the price paid.

However, the vast majority of trade finance transactions (around 80%) are carried out on an open account basis. Open account transactions generally occur where a supplier ships goods to the buyer who then pays for the goods within a period after receipt (which can be on a monthly basis for regular shipments, or as much as 90 days after receipt). They therefore pose considerable challenges for financial institutions seeking to identify TBML, because in a typical open account transaction unless some extra information is included in any associated SWIFT message, there will be limited (if any) information available to the institution over and above the identities of the parties to the payment and the amount to be paid.

In addition to money laundering and other forms of criminality, financial institutions engaged in trade finance must be alert to the possibility that the trade finance they provide could be used as part of a transaction, or series of transactions, designed to evade export controls, to finance nuclear proliferation or to finance terrorism. While this article deals only with TBML, it is clearly vital that firms have systems and controls designed to detect when a transaction involves those additional risks.

Trade Finance and Predicate Criminality

In addition to being a source of significant money laundering and terrorist financing risk for financial institutions, it is worth noting that the same features of trade finance that make it attractive to money launderers also mean that trade finance may be used for a variety of forms of predicate criminality.

Example 1 – Fraud

The paper-based nature of trade finance, and the fact that the underlying trade transactions cross borders makes it an obvious conduit for fraud. Fraud in trade finance transactions may take a variety of forms, including:

- shipping smaller quantities of goods than have been paid for, or goods of a lesser quality; and
- goods have been delivered, but no payment is made.

The difference between fraud in trade finance transactions and trade based money laundering can be found in the fact that trade based money laundering often results from collusion between two parties to a trade finance transaction, whereas fraud is committed by one party to the transaction without the knowledge of the other.

However, the red flags for a fraudulent trade finance transaction can be similar to those for TBML and it may only be as a result of subsequent investigation that a firm is able to categorise a potentially suspicious transaction as one or the other.

Example 2 – Bribery

The payment of a bribe can also be hidden in plain sight through an international trade transaction, and there are various ways that value may be transferred, depending on which way the bribe payment is intended to flow including:

- Under-invoicing – where goods with a greater value are invoiced at a lower rate. This will result in a transfer of value to the purchaser of the goods.
- Over-invoicing – where goods of a lesser value are invoiced at a greater rate, resulting in a transfer of value to the seller.
- Third party payments – where payment is made to, or by, an ostensibly completely unconnected third party.

While customer due diligence measures put in place by firms should detect the direct presence of Politically Exposed Persons (or other high risk individuals) in the transaction, often transactions involving high risk individuals will take place through shell companies of which the person concerned is the ultimate beneficial owner. As such, carrying out appropriate due diligence, and looking for inconsistencies within the transaction itself, will be key in terms of preventing trade transactions being used for bribery.

Regulatory and Law Enforcement Interest in Trade Based Money Laundering

Many regulatory and industry bodies offer practical guidance as to how firms can improve their detection of trade based money laundering, further insight of emerging trends and patterns as well as setting their expectation of the controls firms should already have in place as part of their compliance framework. For UK firms, key guidance has been issued by:

- **The Wolfsberg Group**, which published its updated Trade Finance Principles in January 2017[4].

  The updated principles cover all areas of TBML compliance, including Customer Due Diligence, name screening, financial sanctions, export controls, and the three lines of defence model. It also helpfully includes annexes giving a list of risk indicators and possible controls for different types of trade finance transaction (documentary credits, bills for collection, and standby letters of credit).

  In March 2018, the Wolfsberg Group also released an awareness video on TBML[5]. In doing so, the Group noted that: "Successful mitigation of TBML requires greater collaboration and information sharing between those other key international trade players in the public and private sectors. These include shippers, airlines, truckers, port and customs authorities, businesses and law enforcement agencies."
- **The UK Financial Conduct Authority (FCA)** in 2013, following a thematic review of UK banks' trade finance controls[6].

  The FCA's review noted that TBML controls at banks were generally weak, making key findings relating to: inconsistent approaches to risk assessment; an overall lack of policies and procedures; weaknesses in transaction monitoring and in identifying potentially suspicious transactions for further investigation; a lack of management information; and a scarcity of trade finance-specific training.

  The overall conclusion of the review was that the majority of banks sampled were not taking adequate measures to mitigate the risk of money laundering and terrorist financing in their trade finance business. The annex to the FCA's thematic review provides a number examples of good and poor practice, together with examples of potential red flags as they relate to customers, documents, transactions, shipments and payments.
- **The UK Joint Money Laundering Steering Group (JMLSG[7])**, which issues guidance to UK firms, has issued sector specific guidance relating to trade finance in Chapter 15 of Part 2.

  The JMLSG Guidance on trade finance brings together an explanation of trade finance and how it operates, alongside key compliance activities which Banks should undertake. It explains the difference between different types of trade finance activity, and how they may drive different approaches to matters such as customer due diligence, transaction monitoring and sanctions screening.
- **The Financial Action Task Force (FATF),** which published a detailed study in 2006[8], including a number of case studies of different types of TBML.

  The FATF study focusses on the importance of creating awareness and having strong training programmes to enhance the firm's ability to identify trade based money laundering techniques. It also suggests that firms should be using financial and trade data analysis to identify any anomalies within their data.

  In 2012[9], FATF's Asia Pacific Group produced a further study which set out in more detail a range of potential typologies for TBML, and associated red flags.
- **Bankers Association for Finance and Trade (BAFT)**, which published its guidance on *Combatting Trade Based Money Laundering – Rethinking the Approach in August 2017*[10].

  BAFT focus on alternative approaches to solving the problem of TBML and highlight the misconceptions that have led to the industry struggling to combat this issue. The Annex to the guidance contains a table with a list of red flags and an indication of whether those red flags might appear in open account transactions, documentary transactions, or both.

  The guidance states the importance of pooling resources and information sharing across public and private sectors including customs agencies and financial institutions, in continuing to identify trends and techniques used by criminals to launder money.

  BAFT continue to discuss the leveraging of technologies such as AI and applying data analytics can identify anomalies within data, can allow for a more targeted review of potential illicit activity.

Examples of Trade Based Money Laundering

As set out above, there are few examples of public regulatory action arising as a result of TBML. This is, at least in part, because the complex international nature of TBML and the international trade system makes investigation by regulatory authorities particularly challenging.

Example 1 – Lebanese Canadian Bank

In 2011, FinCEN cited Lebanese Canadian Bank (LCB) as a financial institution of money laundering concern, on the basis that on the basis that accounts held at the bank had been used to channel funds from drug and money laundering schemes (including TBML)

to a number of beneficiaries, including (according to FinCEN) Hezbollah. The scheme centered around purchases of second hand cars in the US – using illegal drug money sent to the US via LCB – that were shipped to West Africa and resold. At the same time, drugs from Colombia were shipped to, and sold in, Europe. The proceeds of sale of the cars and drugs were co-mingled. From there, the funds were sent to exchange houses (some of which held accounts at LCB), which diverted some of the funds to Hezbollah. Finally, LCB's network was also used to transfer funds to Asian producers of commercial goods, to be used for the purchase of goods which were shipped to Latin America and used as part of a black market peso exchange (see below for an example).

FinCEN's notice sets out that while the Bank seemed to be aware of money laundering risk (e.g. through its own risk assessment), it nevertheless permitted hundreds of millions of dollars of illicit funds to be channeled through bank accounts held by individuals suspected of involvement in drug smuggling. FinCEN went on to say that LCB's:

> "*involvement in money laundering is attributable to failure to adequately control transactions that are highly vulnerable to criminal exploitation, including cash deposits and cross-border wire transfers, inadequate due diligence on high-risk customers like exchange houses, and, in some cases, complicity in the laundering activity by LCB managers.*"

FinCEN's designation of LCB as an institution of primary money laundering concern led to civil forfeiture proceedings being taken against LCB, and the Bank eventually closed with its business being acquired by Societe Generale.

Example 2 – Black Market Peso Exchange (BMPE)

The Black Market Peso Exchange has its roots in legitimate trading activity and Colombian Government Policy. Faced with an influx of currency in the 1960s comprising profits from the coffee industry which devalued the Colombian Peso and caused financial instability, the Colombian Government enacted a law which prohibited any Colombian national from holding any currency other than the Colombian Peso. Colombians therefore had two routes to purchase goods abroad: use a bank, which was prohibitively expensive; or turn to an informal means of exchange by which Colombian Pesos were converted to foreign currency by private "brokers".

This system of exchange was exploited by narcotics traffickers wishing to launder significant volumes of currency (normally US Dollars) derived from narcotics trafficking. A narcotics trafficker provides a peso broker with a significant volume of cash, which the broker either then deposits in smaller amounts in US Banks[11], or is held by the broker to pay for goods directly. The funds are then used to purchase goods, which are shipped to South America (normally illicitly) and sold by the broker, whereupon a proportion of the proceeds of sale is remitted to the narcotics trafficker.

In a detailed and useful article on the BMPE[12] in the US Attorney's Bulletin, Evan Weitz and Claiborne Porter[13] set out a number of potential indicators for BMPE activity, including:

- structuring of deposits in round numbers, or just below the reporting threshold for payments into US bank accounts;
- deposits to accounts from multiple locations different from the area in which the account was initially opened, and/or with which the holder of the account has no obvious business link;
- significant volumes of third party payments (often across the counter) into the same account; and
- shipping significant volumes of high value goods, such as perfume and consumer electronics, to South America.

While these indicators are not exhaustive, taken together they could be indicative of an account or a series of transactions requiring further investigation.

Typologies and Red Flags

When considering whether an international trade transaction has potentially suspicious elements, financial institutions will need to consider whether the features of the transaction itself give rise to TBML concerns. As such, it will be vital for the institution to have a suite of potential indicators, or typologies, which reflect the potential risk of TBML to which it is likely to be subject.

Almost all the regulatory and industry guidance given on TBML makes reference to red flags, and many of the documents contain lists of red flags. While it is impossible to produce a truly exhaustive list of red flag indicators, set out below are examples of some of the common red flags[14] that could indicate a suspicious transaction from a TBML perspective:

1. Transaction Inconsistencies

Inconsistencies within the transaction itself can be indicative of potential money laundering risk. When considering the transaction, firms will need to be on the look-out for elements of the transaction that do not make sense in the context of the transaction as a whole, for example:

- customer due diligence processes are unable satisfactorily to verify the existence and ultimate beneficial ownership of entities or other parties involved in the transaction;
- discrepancies in the invoicing for goods and services. Examples might include the weight, amount or quality of the goods being shipped not matching known characteristics of the goods as described on the invoice;
- the market value of the goods being shipped and the overall value of the transaction are not consistent;
- no description of the goods appears on the invoice (this might indicate a phantom shipment);
- the description of the goods does not match international standards or market practice for a particular commodity (e.g. metal shipments of unusually high – or low – levels of purity);
- goods are shipped through a high-risk country when there is no obvious geographic need to do so; and
- there are numerous invoices for the same shipment of goods (this could allow multiple illicit payments, using the invoices as justification).

2. Payments and Third Parties

It will be vital, in terms of controlling TBML risk, for a financial institution to know its customers and to have carried out sufficient customer due diligence. However, even if on-boarding has taken place appropriately, red flags for TBML may arise during the transaction from transactions between related parties, or the involvement of other third parties, or the way payments are made, for example:

- payments in respect of the transaction are made by a third party or made to unrelated third parties;
- there is evidence that funds have been moved to/from accounts in high risk/sanctioned countries;
- transactions have originated from, or passed through, high risk jurisdictions;
- payment has been made of an unusual amount of money (e.g. a much higher, or lower, amount than the transaction would usually require); and

- transaction values do not correspond with a customer's known business (for example, a customer known to deal in small, low value, items suddenly starts concluding transactions for much larger value items).

3. Complex Structures

The use of unnecessarily complex structures for the transaction or in the ownership and management structures of the parties to the transaction may also be indicative of elevated TBML risk. Examples of red flags might include:

- limited information available on the purpose of the business of one or more parties;
- difficulties establishing details of the ownership of one of the parties (either direct ownership or ultimate beneficial ownership);
- suspected shell companies have been identified within the structure. Such companies exist only to reduce the transparency of ultimate beneficial ownership;
- hidden linkages between ostensibly separate parties to a trade finance transaction;
- multiple intermediaries are being used for a transaction for no apparent reason;
- involvement of businesses/parties in a particular jurisdiction is disguised (this may be the case if a transaction is linked with a jurisdiction subject to economic sanctions); and
- concealing the nature of a transaction (for example, a lack of clarity about the economic purpose of the underlying transaction for which trade finance is required). In addition to being a red flag for TBML, this may be indicative of other forms of criminality, including drug trafficking or terrorist financing.

Establishing an Effective Trade Based Money Laundering Compliance Programme

For firms carrying out trade finance activity, establishing an effective control framework addressing TBML will be key to managing legal, regulatory and reputational as risk as part of a wider financial crime compliance programme. It will be vital to ensure that any policies, procedures and controls put in place are reviewed regularly and updated as appropriate, with any changes communicated effectively to affected employees.

An effective TBML control framework will require a number of key elements:

1. A Risk Assessment – Demonstrating an Understanding of the Level of Risk in the Business

One of the central findings in the FCA's Thematic Review was that the practice of incorporating information relating to TBML risk in firms' overall risk assessments, or indeed carrying out a separate TBML risk assessment, was far from universal. The FCA noted that good practice would be for firms to document a trade finance-specific risk assessment that gives appropriate weight to money laundering risk as well as sanctions risk. It also made clear that the failure to keep such a risk assessment up to date would be an example of poor practice.

2. The importance of Knowing Your Customer (KYC)

Given the complex nature of international trade arrangements, and the TBML risk that comes alongside them, undertaking suitable customer due diligence is key to running a successful compliance programme.

Unlike traditional banking relationships, the "customer" in trade finance arrangements will vary depending on the type of arrangement being entered into. As a result, key to any KYC process is understanding which party to the transaction is, in fact, the customer. The JMLSG Guidance contains a number of sections which set out, for certain types of trade finance arrangement, who the "instructing party" is, upon whom appropriate levels of customer due diligence must be undertaken. The guidance goes on to state that where appropriate, and set out in firms' own policies and procedures, it may be necessary to undertake due diligence checks on other parties to the transaction (though the guidance recognises that the extent to which this is necessary will vary).

Where a customer or a transaction is considered to be high risk, the firm concerned will need to carry out enhanced due diligence (EDD) on the instructing party. The JMLSG Guidance explains that EDD measures in trade finance transactions may include obtaining details about the ownership and background of the other parties to the transaction, details as to the type of goods being shipped (including price paid as against market value[15]), frequency of trade, and the quality of the business relationship.

The Guidance goes on to say:

> "*The enhanced due diligence should be designed to understand the nature of the transaction, the related trade cycle for the goods involved, the appropriateness of the transaction structure, the legitimacy of the payment flows and what control mechanisms exist*."

3. Sanctions Screening

Both the Wolfsberg Guidance and the JMLSG Guidance make clear that name screening for sanctioned individuals or entities is a key part of preventing financial crime occurring through trade finance. Interestingly, the FCA's Thematic Review found that sanctions screening during trade finance transactions was among the stronger parts of firms' trade finance compliance frameworks – most likely because firms were already screening transactions for sanctions compliance in any event. The JMLSG goes on to say that where lists are available, firms should consider screening against them in real time.

Both the JMLSG and Wolfsberg guidance note, however, that although screening for sanctioned entities or individuals against sanctions lists is routinely carried out (and many firms have sophisticated electronic systems for doing so), sectoral or goods-based sanctions are far harder to implement, and will require significant expertise, and potentially a more manual approach.

4. Monitoring Customer Activity

All the guidance proposes customer activity monitoring as a key plank in the AML compliance toolkit. However, they are realistic about the extent to which automated transaction monitoring systems are able to detect potential TBML. The JMLSG Guidance makes clear that it will often be difficult to use automated systems due to the fact that the information available varies between the different types of trade finance transaction.

In open account transactions, the level of information may be as little as the identity of the buyer and seller, and the amount to be transferred, posing significant detection difficulties. Several large financial institutions are now exploring whether machine learning or artificial intelligence could be deployed as part of the overall transaction monitoring process to detect patterns in transactions

that might otherwise be missed. While this is something that could prove useful in detecting patterns of illicit activity in open account transactions, further work – and engagement with regulators around the globe – will be vital in determining the extent to which these potential solutions could make open account monitoring more effective in the future.

So while, as the guidance makes clear, the amount and depth of monitoring will depend on the risk analysis of the business or parties involved, in some trade finance transactions (particularly documentary transactions) there is still likely to be a fairly significant manual element, which may well rely on individuals in the business who are responsible for checking documents provided as part of the transaction identifying financial crime risk, based on their knowledge of the industry or of prevailing market conditions. Indeed, the FCA's Thematic Review noted the challenges to firms inherent in this model, particularly given that employees working in trade finance tended to have significant years of experience of doing so – making training of new staff all the more important in terms of the effectiveness of the controls.

5. Training

All the guidance issued by the various standard setting bodies, and the FCA's Thematic Review, make clear the importance of staff being able to access tailored training which is both directed at the staff who deal directly with trade finance issues (and those in the back office), and reflects the risks that trade finance activity represents. In addition to covering the risks of trade finance activity, the training should also cover the firm's procedures for mitigating these risks.

Blockchain – A Use Case?

Many of the inherent risks that financial institutions run in trade finance transactions – the lack of transparency of counterparties, the paper-based nature of the transactions themselves, uncertainties around the provenance and authenticity of products – could be mitigated through the use of distributed ledger technology (or "blockchain") as part of the trade finance process.

In February 2016, Barclays Bank plc released a White Paper[16] which summarised the potential for blockchain technology and its main benefits in trade finance, including:

- mitigating the risk of documentary fraud; and
- providing assurance and authenticity of products in the supply chain.

The Euro Banking Association's Information Paper "*Applying Cryptotechnologies to Trade Finance*"[17] also noted that a blockchain would offer real-time transparency in areas such as payment details, transfer of ownership, the goods themselves, and invoicing. Such transparency would go a long way towards dealing with many of the issues identified in this paper. The Paper also noted that blockchain has the potential to make the whole trade finance process more efficient, for example by improving data matching and reconciliation, enhancing dispute resolution and helping banks themselves manage credit risk by allowing for a more complete risk profile to be generated on clients.

A number of global financial institutions have invested in blockchain trade finance trials, and while at time of writing an industry standard solution seems a fair way off, the results thus far have been promising. Key to any effort to roll out blockchain solutions for trade finance more widely will be regulatory acceptance – as a result, early engagement with regulators around the world is key to ensure that they have a clear understanding of how the solution operates. In doing so it will be key to ensure regulators understand not only the benefits that these solutions may bring in terms of identifying and preventing TBML, but also any new risks to which the solutions may give rise, and how those may be mitigated.

Conclusions

Trade Based Money Laundering poses significant challenges for financial institutions, and while enforcement actions are relatively rare, studies and thematic reviews (such as that carried out in the UK by the Financial Conduct Authority) demonstrate that this is an area in which compliance with regulatory requirements has in the past been weak. And yet, international trade remains an area of significant money laundering and financial crime risk for every firm involved. While the technological solutions, and in particular the potential use of AI and machine learning, and blockchain, seem promising, it will take time to put in place solutions that are adopted widely enough in the industry to make a significant impact on money laundering through international trade. As a result, while firms still often find TBML difficult to detect – "*as if through a mirror, darkly*" – they should continue to invest in their control frameworks as part of a broader financial crime compliance programme, with a view to detecting trade based money laundering, and preventing it where possible.

Endnotes

1. Global Financial Integrity, "*Illicit Financial Flows to and from Developing Countries: 2005-2014*", April 2017, available at: http://www.gfintegrity.org/wp-content/uploads/2017/05/GFI-IFF-Report-2017_final.pdf.
2. For example, letters of credit.
3. These conditions usually relate to delivery of documentation evidencing that the goods have been shipped, such as invoices or bills of lading.
4. Wolfsberg Group, "*The Wolfsberg Group, ICC and BAFT Trade Finance Principles*", January 2017, available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/comment-letters/6.%20Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.
5. See: https://www.wolfsberg-principles.com/articles/launch-trade-based-money-laundering-awareness-video.
6. UK Financial Conduct Authority, "*TR13/3 - Banks' control of financial crime risks in trade finance*", July 2013, available at: https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf.
7. UK JMLSG, Guidance – Part 2, Chapter 15, "*Trade Finance*", December 2017, available at: http://www.jmlsg.org.uk/download/10006.
8. FATF, "*Trade Based Money Laundering*", June 2006, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf.
9. FATF Asia Pacific Group, "*APG Typology Report on Trade Based Money Laundering*", July 2012, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf.
10. BAFT, "*TradeBasedMoneyLaundering*" August 2017, available at: http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paperf246352b106c61f39d43ff00000fe539.pdf?sfvrsn=2.
11. Normally structured in such a way as to avoid the mandatory reporting requirement for US$ deposits over $10,000.

12. Evan Weitz and Claiborne Porter, "*Understanding and Detecting the Black Market Peso Exchange*", US Attorney's Bulletin, September 2013, p29, available at https://www.justice.gov/sites/default/files/usao/legacy/2013/09/16/usab6105.pdf.
13. Claiborne Porter is now a Managing Director at Navigant Consulting in Washington, D.C.
14. The red flags set out below reflect those appearing across guidance issued by the FCA, FinCEN, FATF and BAFT.
15. Interestingly, the Guidance suggests that if the price deviates by more than 25% from market value then further investigation may be warranted. That said, both JMLSG and Wolfsberg recognise that without knowing the precise nature of the goods and the commercial relationship between the parties, it can be extremely difficult to judge whether goods are being shipped at a fair market value.
16. Barclays Bank plc, "*Trading up: applying blockchain to trade finance*", February 2016, available at: https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/product/Banks-Trading-Up-Q1-2016.pdf.
17. Euro Banking Association, "*Applying Cryptotechnologies to Trade Finance*", May 2016, available at: https://www.abe-eba.eu/media/azure/production/1339/applying-cryptotechnologies-to-trade-finance.pdf.

Alma Angotti
Navigant Consulting
Suite 700
1200 19th Street, NW
Washington, D.C. 20036
USA

Tel: +1 202 481 8398
Email: alma.angotti@navigant.com
URL: www.navigant.com

Alma Angotti is a Managing Director and co-lead of the Global Investigations & Compliance practice. A widely recognised AML expert, she has trained and advised the financial services industry and regulators worldwide on AML and CFT compliance. Alma has an extensive background as an enforcement attorney conducting investigations and litigating enforcement actions.

Alma has counselled her clients, global financial institutions and regional institutions, in projects including gap analyses, compliance programme reviews, risk assessments, remediation efforts, and transaction reviews.

Recently, Alma held acting senior AML compliance leadership positions at global and regional financial institutions providing management of their compliance programmes and assisting them with implementing enhancements.

With more than 25 years of regulatory practice, Alma has held senior enforcement positions at the U.S. SEC, FinCEN and FINRA. As a regulator, she had responsibility for a wide range of compliance and enforcement issues affecting broker-dealers, issuers, banks and other financial institutions.

Robert Dedman
Navigant Consulting
Woolgate Exchange, 25 Basinghall Street
London, EC2V 5HA
UK

Tel: +44 207 015 8712
Email: robert.dedman@navigant.com
URL: www.navigant.com

Robert Dedman is a Senior Director in the Global Investigations & Compliance practice. He specialises in government investigations, corporate internal investigations, and anti-bribery and corruption and anti-money laundering compliance projects.

Rob has spent his career immersed in the City of London's Financial Services industry and the workings of the courts and tribunals. He also brings with him a senior regulator's perspective on the supervision of major financial institutions, along with significant expertise in investigations.

Prior to Navigant, Rob worked for the Bank of England, where from April 2013 he set up the Regulatory Action Division – the Bank of England's enforcement and supervisory intervention arm. As Head of that Division, he led the Bank of England's first ever enforcement investigations into misconduct at banks and insurers, achieving significant results against major UK financial institutions, and the first ever prohibition of a Chief Executive of a major bank.

NAVIGANT

Navigant is a publicly traded (NYSE: NCI), international consulting firm with over 5,000 professionals combining sophisticated technical skills with deep industry knowledge to provide customised services that address critical business issues. As an independent consulting firm, Navigant provides its clients with the objectivity and independence they require, without the constraints that accounting firms typically face relative to offering both public accounting and consulting services. Our team includes former senior compliance officers, bankers, accountants, regulators, prosecutors and lawyers, all of whom bring significant experience and deep expertise to help clients build, manage and protect their businesses. The Global Investigations & Compliance Practice, which comprises over 150 professionals worldwide, provides a full range of AML, CFT, anti-bribery and corruption, fraud and financial crime compliance and investigative services to clients across the globe, in the financial services industry and beyond.

Implications of the E.U. General Data Privacy Regulation for U.S. Anti-Money Laundering and Economic Sanctions Compliance

Sharon Cohen Levin

Franca Harris Gutierrez

WilmerHale

I. Introduction

Many financial institutions will confront a new compliance challenge on May 25, 2018, the effective date of the European Union's revamped data privacy law, the General Data Protection Regulation ("GDPR"). In short, GDPR data use *restrictions* conflict with data use *requirements* imposed through U.S. anti-money laundering ("AML") and economic sanctions laws.

The GDPR imposes stringent limitations on processing E.U. residents' personal data. Under this new regime, institutions will be unable to receive, or produce to U.S. authorities or courts, any personal data about their own E.U. customers or customers of their E.U. affiliates *unless* they can identify a GDPR-recognised "lawful basis" to do so. Compliance with U.S. AML and economic sanctions law may require the use of data subject to these restrictions, including customer-identifying information and transaction data. Even though this data is in many cases needed for U.S. law compliance, U.S. AML and economic sanctions laws do not provide an obvious "lawful basis" to process data subject to the GDPR. Navigating these conflicting regimes may expose a financial institution to significant liability if they violate either U.S. or E.U. law.

This article first provides an overview of U.S. AML and economic sanctions laws and the GDPR. The article then analyses the conflicts between the two legal regimes and possible approaches for institutions to minimise such conflicts.

II. The E.U. General Data Privacy Regulation Framework

The GDPR expands upon and replaces the E.U.'s existing data privacy framework, the E.U. Data Protection Directive ("Directive"), to regulate the "processing" of "personal data".[1] While many GDPR requirements align with the Directive, there are significant new provisions in the GDPR, including increased maximum penalties.

A. Covered Data

Under the GDPR, as under the Directive, "personal data" is defined to include any information that could be used to identify any natural person, for example, a name, an identification number, an online identifier, or even location data.[2] Importantly to U.S. AML and economic sanctions obligations, the GDPR regards personal data relating to criminal convictions and offences as particularly sensitive and thus only allows the processing of such information "under the control of official authority or when the processing is authorized by [E.U.] or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects".[3]

B. Restrictions on Processing

In general, personal data is deemed "processed" and thus subject to the GDPR's restrictions any time it is used, collected, retrieved, stored, transferred, disclosed, restricted, altered, or erased, whether through automated processes or manually.[4] The GDPR imposes separate requirements for the processing of data within the European Economic Area ("E.E.A."),[5] the transferring of data from the E.E.A. to locations outside of E.E.A., and the production of personal data to authorities outside of the E.E.A.

1. Processing Data Within the E.E.A.

There are six lawful bases for processing non-sensitive personal data *within* the E.E.A. Those bases are (a) "freely given, specific, informed and unambiguous" consent;[6] and circumstances where processing is necessary, (b) for the performance of a contract with the individual data subject,[7] (c) for compliance with *E.U. or Member State* law, which may include E.U. AML or sanctions laws,[8] (d) for the protection of the life or health of a person (*i.e.*, "vital interests"),[9] (e) for the public interest,[10] or (f) for overriding legitimate interests.[11] Where any one of these bases is present, the processing of personal data within the E.E.A., and the transfer of that data from one place to another place in the E.E.A., are generally permitted.

2. Processing Personal Data Outside of the E.E.A.

For an institution in the U.S. or otherwise outside of the E.E.A. to obtain personal data about its E.U. customers or customers of its E.U. affiliates, additional requirements must often be met. These additional requirements for transferring personal data outside the E.E.A. pose the greatest difficulties for compliance with U.S. AML and economic sanctions laws.

In addition to identifying a lawful basis, additional requirements apply in the following scenarios: (i) an E.U. institution seeks to transfer personal data to a U.S. parent or affiliate; and (ii) a U.S. institution that is itself subject to GDPR (because it serves E.U. residents and markets or monitors customer behavior in the E.U.) attempts to obtain personal data about E.U. customers from *any source*.[12] In either of these scenarios, there must be a lawful basis for the data to leave the E.E.A. *and* the institution receiving the data must be within a country the European Commission deems to offer an adequate level of data protection[13] or must otherwise demonstrate that it adequately protects data. Institutions in countries not deemed "adequate", such as the U.S., must guarantee that they adequately protect data by entering into internal agreements with E.U. affiliate

companies from whom they intend to receive data that contain Standard Contractual Clauses ("SCC").[14] If no such data protection guarantee exists, transfer is permitted only if one or more specified "derogations" exists, for example, explicit informed consent or the "establishment, exercise, or defence or legal claims".[15]

3. Producing Data to Non-E.E.A Authorities and Courts

The GDPR places new restrictions on the production of covered personal data to courts, tribunals, and administrative authorities outside of the E.E.A. – such as the U.S. Department of Justice ("DOJ") and Treasury's Office of Foreign Asset Control ("OFAC"). Under the GDPR, requests or demands for covered personal data from a non-E.E.A. authority, court, or tribunal are not "recognised or enforceable in any manner" unless they are based on an international agreement, such as a mutual legal assistance treaty ("MLAT"), in force between the requesting country and the E.U. or Member State.[16] This requirement is expressly "without prejudice to other grounds for transfer", however, so productions to DOJ or another U.S. authority may still be allowed if a derogation under the GDPR exists.[17]

C. Penalties

The GDPR provides for a maximum administrative fine of €20,000,000 (roughly $25 million) or 4% of the company's "global turnover" (*i.e.*, global revenue), whichever is greater.[18] Before the GDPR, the maximum fine for a data protection violation in most E.U. Member States was under €1 million; even in France, which allowed for a maximum fine of €3 million, the largest fine ever imposed was less than €1 million. The GDPR also allows Member States to impose criminal penalties for certain violations at the discretion of those Member States.[19]

III. U.S. Anti-Money Laundering and Economic Sanctions Framework

Financial institutions in the U.S. are subject to extensive anti-money laundering and economic sanctions laws and regulations. Non-compliance with these requirements can result in significant civil or even criminal penalties.[20]

A. U.S. AML Requirements

The Bank Secrecy Act ("BSA") as amended by the USA PATRIOT Act of 2001,[21] the BSA's implementing regulations,[22] and guidance issued by U.S. regulators establishes the federal scheme of anti-money laundering laws in the U.S. (collectively, the "AML Rules"). The U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") is charged with implementing key aspects of the federal anti-money laundering scheme.

The AML Rules require banks, broker-dealers, and certain other financial institutions[23] operating in the U.S. to serve as a first line of defence against money laundering and terrorist financing. U.S. financial institutions must implement an effective AML program[24] incorporating multiple elements prescribed by regulation.[25] Two of these elements present particular challenges for customers whose data is subject to the GDPR. First is FinCEN's Customer Due Diligence ("CDD") Rule, which became effective on May 11, 2018. The CDD Rule demands that financial institutions collect extensive personal information about their customers and build comprehensive profiles of those customers' behaviour.[26]

Second, financial institutions must also conduct ongoing monitoring of their customers' behaviour. In addition to updating each customer's profile as needed, institutions must file a Suspicious Activity Report ("SAR") with FinCEN any time the institution "knows, suspects, or has reason to suspect" that a transaction that aggregates to $5,000 or more involves illegally derived funds, is designed to evade BSA requirements, or has "no business or apparent lawful purpose". The information needed to perform effective due diligence, monitor customer behaviour, and file SARs will be subject to GDPR restrictions for E.U. customers.

Violations of AML Rules, such as failure to maintain an effective AML program or failure to file SARs, could result in significant civil monetary penalties, fines, and forfeiture. Where the violation of the AML Rules is "willful", institutions and involved individuals may also face criminal penalties.[27] Participation in a money laundering scheme or the knowing receipt of proceeds from criminal activity is also a crime that can result in additional penalties, including imprisonment for involved personnel.[28]

B. U.S. Economic Sanctions Requirements

U.S. financial institutions must also collect personal data about their customers to ensure the customers are not subject to, owned by parties subject to, or affiliated with countries or regions subject to, U.S. economic sanctions programs administered and enforced by OFAC.

OFAC maintains a list of Specially Designated Nationals and Blocked Persons ("SDN") to whom U.S. persons – which includes institutions *and their foreign branches* – may not provide services.[29] Those institutions and branches must routinely screen customers to determine if any customer or certain beneficial owners are subject to sanctions.

OFAC also maintains country-based sanctions programs prohibiting U.S. persons from trading with specific countries or territories, such as Iran, North Korea, Syria, and Cuba,[30] and similar "sectoral" or "hybrid" sanctions relating to Russia and Venezuela.[31] While most sanctions programs apply to U.S. companies and their foreign branches, the Iran and Cuba sanctions programs also apply to *foreign-incorporated subsidiaries* of U.S. companies, meaning that entities in the E.U. must comply with these sanctions programs if their parent is a U.S. institution.[32]

In practice, both list-based sanctions and country-based sanctions require institutions to use information that may be subject to GDPR data use restrictions.

Failure to comply with U.S. sanctions law can result in significant consequences, as OFAC takes a strict liability approach to enforcement. The fines OFAC impose can be substantial, particularly if the involved institution did not "voluntarily disclose" the violation or did not maintain an adequate compliance program or due diligence processes.[33] Where violations are willful, DOJ can impose significant criminal penalties and fines.[34]

IV. Implications

U.S. AML and economic sanctions laws and the GDPR are rife with conflict, and noncompliance with either presents significant risk. It does not help matters that neither the U.S. nor the E.U. recognise the other's law as a legitimate basis for noncompliance with its own regime. The primary implication for financial institutions is that, unless and until solutions arise after GDPR implementation, the conflict between the GDPR and U.S. AML and economic sanctions laws cannot be completely resolved. There are, however, steps financial institutions can take to mitigate the potential impact of these conflicts.

A. E.U. Authorities' Response to U.S. Obligations

E.U. financial institutions can generally rely on E.U. AML and sanctions laws as a recognised "legal obligation" – *i.e.*, one of the

lawful bases – to collect and use customers' personal data within the E.U.[35] The difficulty arises when those E.U. institutions seek to *transfer* such data to U.S. affiliates, or when U.S. institutions subject to the GDPR independently attempt to collect data about E.U. customers. In either of these circumstances, even assuming a Standard Contractual Clause or other recognised legal instrument exists for the transfer of the data to the U.S., it will be difficult for institutions to identify a "lawful basis" for the transfer that E.U. authorities are sure to accept.

Historically, financial institutions have relied on consent when seeking to process personal data covered by E.U. data privacy laws, but the GDPR makes obtaining valid consent considerably more difficult. Under the GDPR, consent must be a "freely given, specific, informed and unambiguous".[36] The GDPR further specifies that "[i]f the data subject's consent is given in the context of a written declaration which also concerns other matters", the data processing consent request must be "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".[37] Further, "[w]hen the processing has multiple purposes, consent should be given for all of them".[38] The GDPR also provides that consent is revocable at any time.[39] Thus, consent is no longer a reliable lawful basis for institutions to collect or transfer large amounts of information about E.U.-resident customers to the U.S. Obtaining consent as a *secondary* basis for the data transfer, however, is often prudent.

The "legal obligation" justification is also precarious. First, the GDPR unequivocally refuses to recognise U.S. law (or any other non-E.U. country law) as a "legal obligation" justifying the processing of E.U. residents' personal data. Thus, E.U. data protection authorities are unlikely to be swayed by an argument that data needed to be transferred to the U.S. to satisfy *U.S.* AML and economic sanctions laws. However, if an institution provides services in the E.U. but conducts its global, enterprise-wide compliance functions out of the U.S., as many multinational financial groups headquartered in the U.S. do, then *E.U.* AML and sanctions laws can arguably provide the "legal obligation" justifying the transfer of data to the U.S. This will be helpful in the AML context, given the substantial overlap between U.S. AML laws and E.U. AML laws; but it will not always help with data transfers to comply with U.S. economic sanctions laws, because OFAC sanctions lists will not always match E.U. and U.N. sanctions lists. Further, it is unclear whether E.U. data protection authorities will accept this invocation of the "legal obligation" lawful basis, given their general scepticism of transfers of data to the U.S.

Absent a clear lawful basis to transfer E.U.-resident customer data to the U.S. under the GDPR, U.S. institutions will have difficulty obtaining the information they need to conduct effective AML programs and to ensure that they and their foreign affiliates do not provide services to individuals and entities subject to OFAC sanctions. U.S. institutions will also have difficulty responding to requests from U.S. prosecutors, regulators, and courts, for documents containing personal data subject to the GDPR, as the GDPR provides that such requests are to be ignored unless procured by MLAT or other international treaty device.

B. U.S. Authorities' Response to E.U. Obligations

In general, U.S. prosecutors and regulators have been sceptical of arguments that U.S. financial institutions could not obtain information needed to effectively conduct AML and economic sanctions monitoring and screening because of E.U. privacy restrictions.[40] Indeed, DOJ and OFAC have pursued U.S. financial institutions even where violations were caused or exacerbated by the fact that the U.S. institution could not obtain customer information from a European affiliate, and DOJ has demanded that U.S. parent companies produce data stored abroad with their subsidiaries in Europe.[41] Institutions that are subject to deferred prosecution agreements have even greater difficulty convincing DOJ to give credence to E.U. data privacy laws; in this scenario, it can appear to the DOJ that the companies are selectively refusing to provide data, and the DOJ will usually insist that the data be produced.

In the past, juxtaposed with DOJ's and OFAC's routine imposition of multi-million-dollar – and in some recent sanctions cases, billion-dollar – penalties, E.U. data protection penalties were often considered trivial. E.U. data protection authorities rarely enforced E.U. data privacy laws and, even when they did, they rarely imposed fines of millions of dollars. U.S.-based financial institutions therefore tended to prioritise compliance with U.S. AML and economic sanctions laws and U.S. authorities' requests for information when they came into tension with E.U. data privacy laws. Relatedly, U.S. financial institutions have typically ultimately acquiesced to DOJ's requests for data stored in the E.U., even if there is arguably a basis to refuse such requests under E.U. data privacy laws. The potential for substantial penalties under the GDPR could alter these dynamics.

C. Steps Forward

The GDPR has and will continue to change the way financial institutions balance their U.S. AML and economic sanctions obligations and their E.U. data privacy obligations, but it is unclear whether it will cause U.S. prosecutors and regulators to revisit their approaches to civil and criminal investigations and penalties. There are some general steps that U.S. financial institutions can take to prepare:

1. *Determine whether your institution is subject to the GDPR.*
   - As a threshold matter, institutions should carefully assess whether any of their U.S. operations are subject to the GDPR by considering whether those operations serve customers living in the E.U. and whether they market in the E.U. or monitor customer behaviour in the E.U.
   - Institutions that conclude that they are not themselves subject to the GDPR should consider to what extent they need to obtain personal information from affiliates in the E.U., for example, affiliates for whom they provide U.S. dollar clearing functions.
2. *Identify a lawful basis for obtaining data from the E.U.*
   - Institutions that conclude that they *are* subject to the GDPR should identify the lawful basis or bases on which they will rely to obtain personal data about E.U. customers.
   - Institutions that conclude that they are not themselves subject to the GDPR, but that need to obtain personal information from affiliates in the E.U., should confirm that the E.U. affiliates have identified a lawful basis to transfer data to the U.S.
3. *Ensure that notice and consent forms are GDPR-compliant.*
   - Because consent may be a lawful basis in certain circumstances, institutions subject to the GDPR or that have E.U. affiliates should ensure that E.U. customers receive customer notice and consent forms that specify that personal data will be transferred to the U.S. to comply with U.S. AML and economic sanctions laws. The forms provided to customers must be unambiguous and not unduly long or complex.
4. *Ensure that adequate data protection safeguards exist.*
   - Institutions should carefully review any existing standard contractual clauses or other data protection agreements

with E.U. affiliates from whom they receive personal data to ensure that the agreements cover all data processing activities in which the institution engages for AML and economic sanctions purposes.

5. *Prepare for prompt notification in the event of a data breach.*
   - Institutions should ensure that they have mechanisms in place to issue data breach notifications to data protection authorities within 72 hours of discovering any such breach and promptly to affected customers.
6. *Appoint a Data Protection Officer.*
   - Institutions subject to the GDPR should appoint a Data Protection Officer to oversee their GDPR implementation and compliance going forward.
7. *Monitor GDPR developments.*
   - The Article 29 Working Party is an advisory body of representatives from each E.U. Member States' data protection authority, the European Data Protection Supervisor, and the European Commission. The Working Party continues to issue guidance concerning the application and interpretation of the GDPR, which should be considered an evolving body of law. Institutions should monitor guidance from the Working Party to ensure that their understanding and implementation of GDPR requirements are up to date.

These recommendations are intended to provide general guidance, but they should not replace more tailored advice focusing on the needs and operations of particular institutions.

V. Conclusion

The GDPR generates new questions and concerns for U.S. financial institutions that directly provide services to E.U. residents or must coordinate their compliance functions with financial institutions in the E.U. Financial institutions' U.S. AML and economic sanctions obligations, which require collection of personal information about customers, is in tension with the GDPR, which generally does not recognise these obligations as a lawful basis to process E.U. residents' data. Although the regulatory environment in both the U.S. and E.U. will evolve upon implementation of the GDPR and much remains unclear, institutions must be aware of these tensions and take certain measures to prepare.

Endnotes

1. Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union ("GDPR"). While E.U. Member States were required to implement the Directive through local implementing statutes (which varied from E.U. Member State to Member State), the GDPR will automatically apply to all E.U. Member States. E.U. Member States will be permitted, however, to enact national legislation to advance specified interests.
2. GDPR Article 4(1).
3. Article 10.
4. *Id.*
5. The E.E.A. includes the countries in the E.U. as well as Iceland, Lichtenstein, and Norway. It remains to be seen whether the U.K. will remain part of the E.E.A. after Brexit.
6. GDPR Article 6(1)(a).
7. GDPR Article 6(1)(b).
8. GDPR Article 6(1)(c).
9. GDPR Article 6(1)(d). *See* Recital 46; Recital 49. This basis would not seem to apply for financial institutions seeking to process personal data in order to ensure AML and economic sanctions compliance.
10. GDPR Article 6(1)(e). *See* Recital 45. The U.K. Information Commissioner's Office ("ICO") guide to the GDPR lists private water companies as an example of an entity that may rely on this lawful basis. *Guide to the General Data Protection Regulation (GDPR)*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ ("ICO Guide"). This basis would not seem to apply to financial institutions seeking to process personal data in order to ensure AML and economic sanctions compliance.
11. GDPR Article 6(1)(f).
12. GDPR Article 44; GDPR Article 45; Recitals 78–91.
13. *See* GDPR Article 45; Recital 103.
14. GDPR Article 46.
15. GDPR Article 46. For accepted derogations, *see* GDPR Article 49(1).
16. GDPR Article 48.
17. *See* GDPR Article 48; GDPR Article 49.
18. GDPR Article 83(4)-(5).
19. *See* GDPR Article 84(1).
20. *See* 31 U.S.C. § 5321; 31 U.S.C. § 5322; 31 CFR Appendix A to Part 501; 12 CFR § 12.21; 12 CFR § 21.11; 12 CFR § 163.180.
21. *See* 31 U.S.C. § 5311 *et seq*.
22. *See* 31 C.F.R. Subt. B, Ch. X.
23. 31 U.S.C. § 5312(a)(2) and (c)(1). *See* 31 C.F.R. § 1010.100(t).
24. *See* 31 U.S.C. § 5318(h); 31 C.F.R. § 1010.210. *See also* Fed. Fin. Inst. Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual 28 (2014) ["FFIEC Examination Manual"].
25. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29420 (May 11, 2016) (codified at 31 C.F.R. § 1010.230) (describing the "five pillars" of an effective AML program) ["CDD Rule"].
26. *See* CDD Rule, 81 Fed. Reg. 29398. A bank must file a Suspicious Activity Report ("SAR") with FinCEN any time the bank "knows, suspects, or has reason to suspect" that a transaction that aggregates to $5,000 or more involves illegally derived funds, is designed to evade BSA requirements, or has "no business or apparent lawful purpose". 31 C.F.R. § 1020.320. Other financial institutions are also subject to specific SAR requirements.
27. 31 U.S.C. § 5321; 31 U.S.C. § 5322;12 U.S.C. § 1818(i); 31 C.F.R. Appendix A to Part 501.
28. 12 U.S.C. § 1956; 12 U.S.C. § 1957.
29. OFAC Specially Designated Nationals and Blocked Persons List, https://www.treasury.gov/ofac/downloads/sdnlist.pdf (last updated Apr. 6, 2018).
30. *See* Sanctions Programs and Country Information, U.S. Dept. of Treasury, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx (last updated Apr. 6, 2018).
31. *See e.g.*, Executive Order 13662 (Mar. 20, 2014); Executive Order 13808 (Aug. 24, 2017).
32. 31 C.F.R. § 560.215; 31 C.F.R. § 515.329. *See also* OFAC FAQ, U.S. Dept. of Treasury, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx.

33. *See, e.g.*, *Settlement Agreement Between U.S. Dep't of the Treasury, Office of Foreign Asset Control, and Crédit Agricole Corporate and Investment Bank*, COMPL 1000368 (Oct. 15, 2015), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib_settlement.pdf (settling for a $330 million fine for egregious violations not voluntarily disclosed).
34. *See* 50 U.S.C. § 1705. *See also* Press Release, U.S. Dep't of Justice, *ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran* (Mar. 7, 2017), https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending (imposing a combined penalty of $1.19 billion with Dep't of Treasury and Dep't of Commerce).
35. Indeed, the U.K. ICO's Guide on the GDPR specifies that a financial institution may "rel[y] on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 [one of the U.K.'s chief anti-money laundering laws] to process personal data in order submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering". ICO Guide, *supra* note 22.
36. GDPR Article 4(11).
37. GDPR Article 7(2). *See also* Recital 42.
38. Recital 32.
39. GDPR Article 7(3). Any processing that occurred pursuant to consent and before that consent was revoked remains valid, however. *Id.*
40. *See, e.g.,* Remarks by Assistant Attorney General for the Criminal Division Leslie R. Caldwell at the 22nd Annual Ethics and Compliance Conference, Oct. 1, 2014, https://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics.
41. *See U.S. v. Microsoft Corp.*, No. 16-402, On Writ of Certiorari to The United States Court of Appeals for The Second Circuit. The question in this case is whether the DOJ can compel Microsoft to produce documents it has stored on servers in Ireland maintained by its Irish subsidiary.

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Bradford Hardin (counsel), Jacquelyn L. Stanley (senior associate), Zachary Goldman (senior associate), and Nicholas Simons (associate). The WilmerHale lawyers are members of the Regulatory and Government Affairs Department and the AML and Economic Sanctions Compliance and Enforcement practice.

Sharon Cohen Levin
WilmerHale
7 World Trade Center, 250 Greenwich Street
New York, New York 10007
USA

Tel: +1 212 230 8804
Email: sharon.levin@wilmerhale.com
URL: www.wilmerhale.com

Sharon Cohen Levin is a leading authority on anti-money laundering (AML), Bank Secrecy Act (BSA), economic sanctions and asset forfeiture. She served for 19 years as Chief of the Money Laundering and Asset Forfeiture Unit in the US Attorney's Office for the Southern District of New York (SDNY). Under her leadership, the SDNY forfeited in excess of $15 billion. During her tenure at SDNY, Ms. Levin prosecuted and supervised many of the Department of Justice's most complex and significant money laundering, sanctions and asset forfeiture prosecutions. Since joining WilmerHale she has represented a diverse array of financial institutions with respect to AML and sanctions issues, including developing AML and sanctions programs and counseling clients on AML and sanctions compliance. Ms. Levin represents individuals and institutions in criminal, civil and regulatory investigations and enforcement actions.

Ms. Cohen Levin's full professional profile is available at: https://www.wilmerhale.com/Sharon_Levin/.

Franca Harris Gutierrez
WilmerHale
1875 Pennsylvania Avenue
Washington, D.C. 20006
USA

Tel: +1 202 663 6557
Email: franca.gutierrez@wilmerhale.com
URL: www.wilmerhale.com

Franca Harris Gutierrez, a Partner and Vice Chair of the Financial Institutions Practice Group. Ms. Harris Gutierrez, who joined the firm from the US Department of the Treasury's Office of the Comptroller of the Currency (OCC), leads one of the country's preeminent banking and financial services practices. She advises clients on complex anti-money laundering issues arising in regulatory, enforcement, and transactional contexts. Maintaining an active enforcement practice, she defends clients before all the federal banking agencies and other federal and state enforcement bodies including the New York Department of Financial Services. She is a leader in a number of financial institutions spaces and counsels a broad range of US and non-US financial institutions.

Ms. Harris Gutierrez's full professional profile is available at: https://www.wilmerhale.com/franca_gutierrez/.

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WilmerHale's interdisciplinary AML and Economic Sanctions Compliance and Enforcement Group brings together leading practitioners to focus on our clients' most challenging AML- and economic-sanctions-related regulatory, examination and enforcement issues. The team has a wealth of knowledge and government experience at the forefront of AML and sanctions policy and enforcement. Our lawyers have worked in the US Department of Justice, US Attorneys' Offices, the US Department of the Treasury, the US Department of State, the Central Intelligence Agency and the National Security Agency, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the White House, and the United States Congress. This depth of experience enables us to assist clients in anticipating and understanding the government's priorities, communicating with regulators and key stakeholders, and resolving their most challenging matters and law enforcement proceedings.

Navigating the AML Compliance Minefield

Norman Harrison

Kathy Malone

Duff & Phelps, LLC

Introduction

Anti-money laundering (AML) enforcement presents a mounting risk and compliance burden for financial institutions as well as other businesses that conduct cash-based transactions. Over the past decade, enforcement of AML regulations has grown far more stringent. Financial penalties have mushroomed, and regulators are increasingly holding executives personally responsible for non-compliance. Meanwhile, the financial industry's exposure to money laundering is vast. An estimated 2% to 5% of global GDP is laundered every year.[1] Much of this cash enters the international banking system.

The vigor of enforcement, the broad scope of conduct that constitutes money laundering, and the challenges of compliance add up to a serious risk for financial institutions. By extension, there is also a risk to their directors, executives and shareholders. Money laundering is so common that no financial institution can safely doubt they are at risk or adopt a casual approach to AML compliance.

While it is too early to know exactly how the Trump Administration might alter AML enforcement, there is ample reason to believe the current trend of vigorous enforcement will persist. The administration's agenda of reducing the regulatory burden likely will be offset in the AML arena by an emphasis on fighting terrorism, drug trafficking and other international crimes.

Official statements regarding other categories of financial wrongdoing suggest the administration will continue to emphasise both strict enforcement and individual accountability. These statements include the approach to securities enforcement espoused by Securities and Exchange Commission (SEC) Chairman Jay Clayton, as well as the new guidelines on Foreign Corrupt Practices Act (FCPA) enforcement announced last fall by Deputy Attorney General Rod Rosenstein. Likewise, both the SEC and the Financial Industry Regulatory Authority (FINRA) have identified AML compliance as a continuing enforcement priority for 2018.

In conversations with our firm, executives and officials who hold AML responsibilities have understandably expressed concerns. While regulatory relief on AML is unlikely, in our experience there are various steps companies can take to minimise the risk of money laundering. This article examines current trends in AML enforcement and provides observations on best practices available to financial institutions to measure and mitigate risks. While we believe these observations are applicable to most businesses that face AML risks, we recognise each company's situation is unique, and there is no substitute for targeted professional advice.

Trends in AML Enforcement

As noted above, AML enforcement has escalated in recent years. This escalation has taken several forms: holding individuals personally liable for compliance failures and the underlying conduct; imposing greater financial penalties; emphasising an admission of wrongdoing; and targeting a broader scope of money service companies, and even vendors, for AML non-compliance. Moreover, compliance expectations are mounting. For example, the new "beneficial ownership" Customer Identification Program (CIP) rules going into effect in May 2018 will require companies subject to Bank Secrecy Act[2] (BSA)/AML rules to identify individuals who hold more than a 25% interest in customers structured as entities. This section addresses each of these trends.

Individual Liability: Since the financial crisis, financial regulators have stressed their intention to hold individuals accountable for wrongdoing. In AML compliance, this has resulted in notable enforcement actions against corporate officials. In May 2017, for example, FinCEN secured its largest ever fine against an individual, a $250,000 civil penalty against a chief compliance officer for failing to implement an effective AML programme. The settlement included an admission of guilt and a three-year injunction barring the officer from performing a compliance function.[3] It marked only the second time in FinCEN's history that it sued to enforce a monetary penalty.[4] The case set an important precedent in which a federal district court reaffirmed that regulators were authorised to impose monetary penalties against officers of financial institutions. Despite concerns that such penalties would have a chilling effect on the compliance profession,[5] FinCEN stated that individual liability "strengthens the compliance profession by demonstrating that behavior like this is not tolerated within the ranks of compliance professionals".[6]

Corporate Financial Penalties: The Congressional Research Service (CRS) recently reported a significant escalation in both the frequency and size of corporate AML penalties since 2012. Citing a National Economic Research Associates study,[7] CRS noted that from 2012 through to 2015 nearly 90% of AML enforcement actions included financial penalties, compared to less than half between 2002 and 2011, and that "more than 80% of total money penalties imposed for BSA/AML violations since 2001 have been levied after 2012". The CRS report also noted that "since October 2009, nearly one-third of BSA/AML penalties have exceeded 10% of a defendant institution's capital. By contrast, no penalty imposed before 2007 exceeded 9% of a defendant institution's capital".[8]

Admission of Wrongdoing: Regulators have increasingly required an admission of wrongdoing to be an important element of resolving enforcement actions. As former FinCEN director Jennifer Shasky Calvery stated in her remarks to the American Bankers Association/

American Bar Association Money Laundering Enforcement Conference, "Acceptance of responsibility and acknowledgment of the facts is a critical component of corporate responsibility".[9] This contrasts with pre-crisis practices and raises reputational risks. It also creates increased litigation risk for institutions that settle AML prosecutions. Required admissions have applied both to individual compliance officers and corporations. The two largest monetary penalties, both assessed against major financial institutions, have included acceptance of wrongdoing.[10] In some cases, regulators have even required a sanctioned compliance officer to disclose the enforcement action to future employers.[11]

Broader Scope of Compliance: Another clear message from regulators and law enforcement is that the range of entities subject to AML laws and regulations is broader than has sometimes been understood. Regulators have underscored that virtually any money services business can be held accountable. Additionally, several federal agencies have recently released guidance on corporate liability arising from third-party relationships, including vendors, for violations caused by the third party. Under 2017 Office of the Comptroller of the Currency guidance, for instance, potential enforcement targets could include mortgage servicers, software providers and even independent auditors.

Another trend regarding culpability involves an increasing tendency of prosecutors to infer wilfulness, or intent to violate BSA/AML requirements, from the resources an institution devotes to compliance. One vivid example is the 2017 prosecution of a firm in which wilfulness was inferred from the paucity of resources devoted to AML compliance. Some examples include running only two scenarios to identify risky transactions, generating only paper reports for a business that engaged in almost $9 billion of money transfers annually, and filing only nine SARs out of a total of 18,000 alerts the bank's system had triggered as warranting further review.[12]

Beneficial Ownership Rule: Finally, trends in enforcement and investigations over the past several years have shown heightened expectations around the customer due diligence process, particularly following revelations from the Panama Papers controversy. FinCEN has issued a new "look through" rule that requires financial institutions subject to the BSA to identify the beneficial owners of customers organised as shell companies and other entities they do business with. The new rule, which carries a compliance deadline of May 11, 2018, defines a beneficial owner as any individual holding an ownership stake of 25% or more of a company. Practitioners are eagerly awaiting the issuance of regulatory guidance on the new rule, which is lengthy and complex.

Key Steps for AML Compliance

The most effective way to navigate this more stringent AML landscape is to avoid the enforcement minefield altogether. This means complying with the spirit and letter of the law and meeting regulatory expectations. Regulators have stressed that an *intent* not to break the law is not an adequate defence, nor is ignorance of a customer's activities or subcontracting AML compliance to a vendor. Instead, the onus is on the firm to demonstrate that it has built an AML compliance programme sufficiently robust to address the risks posed by its business and customers.[13]

In brief, there are three pillars to implementing a robust compliance programme:

1. the programme must be based on a detailed, well-executed risk assessment;
2. it must designate and faithfully implement compliance procedures tied to the risks identified in the assessment and report any suspicious activity promptly to regulators; and
3. the programme must undergo regular and ongoing review, testing and evaluation.

Within this framework, the following describes best practices that firms should consider.

Get Your Risk Assessment Right

Risk assessment is the first pillar of AML compliance and is the backbone of any AML compliance programme. Defining and evaluating potential risks is a crucial first step towards building an effective compliance programme. In other words, a company can't manage what it doesn't measure. In the event that wrongdoing occurs, regulators and prosecutors often view a failure to conduct an adequate risk assessment as being more culpable than not conducting one at all. Moreover, the assessment should be updated whenever there is a material change to the business, such as through a merger, acquisition, substantial geographic or operational expansion, or a change in customer base that significantly changes the company's risk profile.

Attention to detail is vital. A covered institution should ensure the individuals conducting the risk assessment have the background, skills and resources required to identify all of the firm's potential risks. The assessment team should be empowered by a mandate from the C-suite to promote cooperation. The team should examine all entities and lines of business subject to AML regulations, reviewing documents and conducting interviews with key personnel. It should consider such factors as: location; type of entity; and the degree of difficulty in conducting due diligence and determining the beneficial ownership of clients or customers, in accordance with local laws and regulations. The risk assessment should document risks and flag businesses and geographies where money laundering activities are particularly prevalent. Regulators have underscored the importance of evaluating the unique risks posed by a business and of identifying reasonable controls. Failing to do this has been characterised as an "unacceptable risk" of AML non-compliance.[14]

Using the information gathered during the research phase of the risk assessment, the firm should develop a scoring system (for example, by line of business, geography, customer category or individual customers) to help the firm's compliance personnel target their surveillance efforts. A well-executed risk assessment should also be sufficiently forward-looking to prepare the firm for external review of the compliance programme. For example, it should identify areas of focus for testing transactions and for reviewing client files and other records for later evaluation of the programme. Finally, the risk assessment should be sufficiently thorough and well designed to persuade regulators that the firm has invested adequate time and resources in its efforts to identify potential money-laundering activities.

Ensure Appropriate AML Leadership, Staffing and Reporting

The second pillar of AML compliance, effective implementation, relies largely on the personnel charged with day-to-day oversight of the programme. Ideally, the AML compliance officer should be an experienced, board-selected expert in AML. The compliance officer should also have access to outside professional assistance, particularly if the individual does *not* have significant AML expertise. Moreover, the compliance team should have a budget that enables it to carry out its mandate, and the budget should adapt to changing conditions within the institution or in its competitive or geographic environments. The AML compliance budget should keep pace with the demands of a growing institution, especially one that has acquired new lines of business.

It should be stressed that the AML compliance officer, or designee, is responsible for reviewing and signing off on all AML-related documentation. This is a time-consuming, yet critical, responsibility. Duff & Phelps has found that a failure to comply with this requirement can raise red flags, triggering enforcement action.

Address Hurdles to Collecting Know Your Customer (KYC) Documentation

A common barrier to effective AML compliance is an unwillingness of clients and customers to share documentation needed to fulfil the KYC requirements that are a cornerstone of the AML regulations.

Typically, for instance, a covered institution will request a company's articles of incorporation as evidence that a business exists as a legal entity. If the client is reluctant to provide its articles, it often helps for the relationship manager and/or the firm's AML compliance vendor to provide an explanation, clarifying why the information is needed.

Alternatively, AML regulations allow for a variety of acceptable documents in cases where customary documentation is unavailable. For example, *in lieu* of articles of incorporation, a company may submit a government-issued business licence, a partnership agreement or a trust instrument. This is not an exclusive list. FINRA has clarified that a financial institution "may use other documents for verification provided that the documents allow a firm to establish a reasonable belief that it knows the true identity of the customer".[15] FINRA encourages firms to obtain "more than one type of documentary verification to ensure that they have a reasonable belief that they know their customers' true identities".[16] Multiple forms of verification increase the likelihood of identifying inconsistencies that might raise red flags. Extra care should always be taken in cases involving politically exposed persons and particularly with senior foreign political figures, who should *always* be subject to enhanced due diligence under AML regulations.

If a prospective client remains unable or unwilling to comply with basic information requests even after the financial institution clarifies why the documentation is needed, and offers alternative documentation options, the firm would typically be advised *not* to do business with the client. The willingness of a financial institution to decline potential clients, particularly major ones, who are unable to satisfy KYC requirements is a critical measure of whether its compliance programme is truly robust.

Consider Outsourcing Judiciously

The decision of whether to outsource all or some elements of an AML compliance programme is a complex, firm-specific decision. Many firms choose to retain outside expertise to assist with certain aspects of the programme, such as training employees and, as discussed above, conducting risk assessments, and reviewing and testing compliance programmes. Firms often outsource in circumstances where they don't have adequate time or resources to hire and train a full-time compliance team. Some may choose to outsource a significant part of the programme when they face business constraints, such as a new acquisition that dramatically changes the risk profile.

If the firm selects a professional, seasoned consultant, it benefits from a well-trained, well-equipped team on day one. Moreover, when comparing the cost-effectiveness of maintaining expertise in-house *versus* contracting with a specialist, many firms find compelling cost efficiencies to outsourcing. It should be stressed, however, that outsourcing a compliance programme does *not* shift the ultimate compliance responsibility to the vendor, regardless of the vendor's reputation or track record. If a violation occurs, regulators will still hold the firm accountable. Hiring a reliable consultant with a strong track record may boost the credibility of the compliance programme with regulators.

Regularly Conduct Independent Compliance Programme Testing

The third pillar of robust AML compliance is an obligation to conduct ongoing review, testing and evaluation of the compliance programme. A continuous process of evaluation and testing of the AML compliance programme is an essential feature of an effective programme. (This is true also with respect to compliance efforts relating to the FCPA, sanctions, anti-terrorist financing and other financial crimes.) In our experience, this is a requirement that deserves extra vigilance, as it is an area where regulators often find that firms fall short.

While the law allows for independent reviews to be conducted internally, retaining a consultant to conduct periodic assessments of the effectiveness of an AML compliance programme reduces the risk of conflicts or appearances of conflict. It is especially important to construct a framework in which the assessment is conducted by persons not associated with the businesses being evaluated. Some institutions rely on their internal audit team to develop the expertise needed to evaluate compliance programme effectiveness; while others engage external consultants to conduct an independent review, or at least to train and support internal audit personnel in these efforts. Such consultants should have deep experience in testing AML programmes and should be independent of the firm hired to handle compliance. The team conducting the review should have a direct reporting line to senior management, as well as to the audit committee or independent directors in a public company.

Provide Open Communication Channels for Whistleblowers

Regulators are inundated with thousands of SARs each year. As such, some of their most promising AML enforcement leads may arise from employee tips, independent of official compliance channels. Such tipsters, who may in some cases benefit from federal whistleblower incentives, can put even the most diligent company compliance office in a difficult situation. As such, companies are advised to cultivate a culture where employees are encouraged to bring suspicions or evidence of wrongdoing to the relevant compliance officials in the first instance.

The company's compliance policies should set the right "tone at the top", including clear guidance on how to submit tips. The company should also publicise a strict anti-retaliation policy, noting that employment law assigns criminal penalties for retaliating against whistleblowers. While statutes prohibit discouraging a tipster from filing a report with law enforcement, companies can diminish the odds of escalation by stressing that the tip is welcomed and will be taken seriously. A well-administered anonymous tip programme can also help by providing a channel for employees who may not be comfortable coming forward in person, especially if a hotline or anonymous e-mail reporting channel is administered by a third party rather than by the company itself.

Think Like a Regulator

Regardless of how robust a firm's AML efforts are, what matters most in avoiding the enforcement minefield is how regulators view the implementation and effectiveness of a compliance programme.

Generally speaking, with regulators *the rule is the rule*. If a firm is required to collect documentation and it doesn't consistently do so, it is liable to suffer enforcement action. Attempting to show that, despite lapses, the firm has a strong programme may have a minor mitigating effect, but it is unlikely to keep enforcement at bay.

Be Proactive About SARs

Regardless of the effort and resources dedicated to a compliance programme, many enforcement actions are rooted in a firm's failure to file SARs with sufficient diligence, timeliness and consistency. This, therefore, is a key area for monitoring and measuring by the compliance team. Regulators receive thousands of SARs each year. In general, if a firm suspects it *might* need to file a SAR, it probably should do so. Financial institutions that proactively alert regulators to problems can generally expect more favourable treatment in terms of fines or other sanctions in the event of wrongdoing.

Establish an Expansive AML Training Programme

Training is an essential element of an effective AML compliance programme and a key expectation within AML regulations. When examiners review a firm's programme, training is typically one of the areas they inspect. Compliance officials should review the programme regularly to confirm it is up to date with the law, enforcement priorities and the firm's mechanisms and risk profile. All relevant employees should be trained in AML compliance, and the firm should have a certification requirement to ensure that all required employees fulfil this obligation. Additionally, employees in specific risk categories should receive more frequent and detailed training.

Computer-based training programmes can help streamline this expectation and can track fulfilment. In addition to providing the necessary information and guidance, training should underscore a culture of compliance. Finally, training compliance should be reviewed regularly, particularly when employees change jobs.

Look for Potential Conflicts of Interest

Finally, we note that client-facing employees who earn commissions or performance bonuses, based on assets under management, have an incentive to overlook the suspicious activities of a large client. For many firms, this poses a vulnerability, and one that may be difficult to address.

A strong, well-designed compliance structure can help. Many firms establish incentives for the compliance team that are not tied to profits. Others embed compliance personnel in operating units to have an ongoing presence, with the goal of reducing tensions and fostering cooperation. The firm's messaging and conduct should indicate to the revenue-generating personnel that the compliance team is not the enemy and that both teams share a common goal: the health, success and prosperity of the business. Finally, particularly given the current aggressive enforcement climate, firms are advised to enforce a well-publicised zero-tolerance policy for employees who put financial incentives ahead of regulatory obligations.

Conclusion

Under an increasingly rigorous and expansive AML enforcement regime, all financial institutions and money service firms are advised to implement a robust compliance programme to minimise the risks and potentially mitigate or altogether avoid large financial penalties and personal liability. The steps outlined in this article can help companies to achieve these goals by maintaining vigorous and effective compliance efforts, and by monitoring and adapting to changes in applicable laws and regulations. Every institution that faces money laundering risks should obtain the necessary expertise and carefully tailor its compliance programme to the specific risks it faces.

Endnotes

1. https://www.unodc.org/unodc/en/money-laundering/globalization.html.
2. BSA is the Bank Secrecy Act, which governs anti-money laundering regulations on financial institutions.
3. https://www.fincen.gov/news/news-releases/fincen-and-manhattan-us-attorney-announce-settlement-former-moneygram-executive.
4. https://www.bakerdonelson.com/trends-in-anti-money-laundering-enforcement-and-compliance.
5. https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubID=17179883478.
6. https://www.fincen.gov/news/news-releases/fincen-and-manhattan-us-attorney-announce-settlement-former-moneygram-executive.
7. http://www.nera.com/publications/archive/2016/developments-in-bank-secrecy-act-and-anti-money-laundering-enfor.html.
8. https://fas.org/sgp/crs/misc/R45076.pdf.
9. https://www.fincen.gov/news/speeches/remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-7.
10. https://fas.org/sgp/crs/misc/R45076.pdf.
11. Anti-Money Laundering Enforcement: The Rise of Individual Liability for Compliance Professionals; Securities and Commodities Regulation, Vol. 49 No. 21 December 7, 2016.
12. https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations.
13. https://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html.
14. https://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html.
15. http://www.finra.org/sites/default/files/NoticeDocument/p003246.pdf.
16. http://www.finra.org/sites/default/files/NoticeDocument/p003246.pdf.

Norman Harrison
Duff & Phelps, LLC
555 12th St. NW, Suite 600
Washington, D.C. 20004
USA

Tel: +1 202 649 1200
Email: norman.harrison@duffandphelps.com
URL: www.duffandphelps.com

Norman Harrison is a managing director at Duff & Phelps based in Washington, D.C. Norman has over 25 years of experience advising companies on internal investigations, regulatory compliance and fiduciary duty issues, and transactional support (including due diligence and post-acquisition disputes). He has also led multi-disciplinary teams in DOJ and SEC independent monitoring appointments. Norman has conducted numerous internal investigations in matters arising from federal investigations, shareholder allegations, media exposés and other circumstances. He also has extensive experience relating to compliance consulting and monitoring, including in matters involving bribery, corruption, money laundering and other financial crimes. Norman has advised boards of directors and developed expert testimony on fiduciary duty and corporate governance issues. He also has substantial experience in risk management, operations, fiduciary duty and compliance issues, and dispute resolution involving investment funds. Norman holds a B.S.B.A. in Finance from Georgetown University and a J.D. from Georgetown University Law Center.

Kathy Malone
Duff & Phelps, LLC
1 Landmark Square 18th Fl
Stamford CT 06901
USA

Tel: +1 203 900 0501
Email: kathy.malone@duffandphelps.com
URL: www.duffandphelps.com

Kathleen Malone is an attorney and a managing director at Duff & Phelps based in Stamford. Kathleen has worked with a number of private fund managers in registering them with the appropriate regulatory authority, establishing compliance programmes, identifying and addressing risks and conflicts, conducting mock regulatory examinations and assisting with regulatory examinations and inquiries. In addition, Kathleen has assisted several broker-dealers with their regulatory needs from registration, to ongoing compliance support, FINRA examination support, as well as the testing of their compliance programmes. During Kathleen's more than seven-year tenure at the SEC, she worked in the New York and Boston Regional Offices, where she participated in numerous, registered investment company, registered investment adviser and broker-dealer examinations. Throughout her tenure at the SEC she participated in examinations of a wide variety of registered entities including hedge funds, mutual fund complexes, investment advisers and jointly registered investment advisers and broker-dealers.

DUFF & PHELPS

Protect, Restore and Maximize Value

Duff & Phelps is the global advisor that protects, restores and maximises value for clients in the areas of valuation, corporate finance, disputes and investigations, compliance and regulatory matters, and other governance-related issues. When companies, funds or legal teams need to synthesise complex data sets, identify important matters of fact or quantify damages, they hire Duff & Phelps. Our team of valuation, corporate finance, forensic accounting and regulatory experts help clients diagnose and resolve complex business challenges in every region of the world and across all industry sectors. We bring all the resources of a truly integrated global team for client disputes. Duff & Phelps provides confidential consulting services, as well as expert testimony. Duff & Phelps has decades of experience investigating corporate wrongdoing and associated controversies, including theft, broken deals, post-acquisition disputes and a wide range of financial, accounting and other frauds. We have scrutinised cases involving a broad array of regulatory and criminal authorities, including the SEC, DOJ, FINRA, IRS, and FTC, along with state regulators and prosecutors, as well as enforcement authorities around the world. Our professionals include former officials and agents from the SEC, FBI and CIA who provide invaluable insight into how government investigators think and the investigative processes they employ. As a global firm offering a broad array of independent advisory services, we serve more than 5,000 clients each year, including over 50% of the S&P 500, 80% of the Am Law 100 and 70% of the world's top-tier hedge fund and private equity funds. The firm's nearly 2,500 professionals are located in over 70 offices in 20 countries around the world. For more information, visit www.duffandphelps.com.

Best Practice in AML/KYC Compliance: The Role of Data and Technology in Driving Efficiency and Consistency

Wayne Johnson

Joel Lange

Encompass & C6 an Acuris Company

Regulation stops for no one. Regulated firms are still reeling from the European Union's Fourth Money Laundering Directive (4MLD), and with 5MLD hot on its heels, the pressure to adapt anti-money laundering (AML) and know your customer (KYC) processes shows no sign of abating. This drive is not surprising: in the UK, for example, the National Crime Agency recently announced that its previous GBP 36–90 billion figure for all money laundering impacting on the UK is a significant underestimate[1]. And with the 2017 UK Criminal Finances Act[2] introducing new corporate criminal offences for failing to prevent facilitation of UK and foreign tax evasion, the pressure is rising on businesses to ensure they don't fall foul of the new legislation. Across the globe, governments are uniting in a bid to protect the financial system from facilitating organised crime and corrupt behaviour.

As a consequence of the Panama and Paradise Papers revelations, legal and professional services firms have also come under increased regulatory scrutiny as potential "professional enablers" of financial crime. The UK's Solicitors Regulation Authority (SRA) has stated that money laundering is a key focus area, and the National Crime Agency's "Flag It Up"[3] campaign highlights the attention this sector can expect in the coming years.

The financial sector has led the way in implementing robust AML and KYC programmes. Billions of dollars have been invested in the people, data and technology needed to fully identify, assess and mitigate regulatory risk. This level of spend, and the sheer number of people employed in compliance-related roles, can make it seem like achieving robust compliance is out of reach for any firm that is just setting out on the journey. However, it's important to remember that financial institutions started out on the road to compliance in a very different environment. The data needed to fully assess risk was far harder to access a decade ago, and technology has advanced beyond expectations.

Today, information required for KYC is available as digitised streams from a broad range of primary and secondary sources. For many companies, the stumbling block is creating an affordable KYC process that harnesses the best information to create risk assessments that are fully documented, up to date, and available to regulators and the firm's authorised risk professionals. Today, advances in technology mean that effective compliance can be implemented at a fraction of the cost, and with much smaller teams.

This article outlines the challenges of the most recent AML and KYC regulations, highlights the practices that give firms maximum protection from risk and presents a modern approach to compliance.

4MLD – Key Points

4MLD has placed a tremendous burden on regulated firms, who have to review existing policies and procedures and remediate KYC profiles to comply with it. The incoming 5MLD regulation, which we discuss later, adds turbulence, compelling firms to deal with two significant regulatory events in a short space of time.

Risk-based approach

While the concept of a "risk-based" approach to AML/KYC compliance is not new, 4MLD places far more emphasis on it than before. Regulators now expect to see intelligent and effective compliance that is focused on mitigating risk, not a tick-box exercise that puts every customer through the same level of due diligence regardless of their risk profile.

There is, however, an upside to a risk-based approach. It means limited resources can be focused on the areas of greatest risk, saving time and cost and maximising the effectiveness of a compliance programme. By spending less time on low-risk customers, teams are freed up to focus on more complex cases, where they can dig deeper to uncover hidden risks.

Ultimate Beneficial Owners (UBOs)

Because corporate vehicles provide excellent cover for individuals attempting to launder money or evade tax, the requirements in 4MLD to fully understand a customer's corporate hierarchy and ownership structure are more onerous than before. The regulation demands that all EU Member States publish and maintain public registries of beneficial ownership covering individuals who ultimately own or control more than 25% and one share of a company. These registries will be interconnected to increase cooperation between Member States and to improve the ability to detect potential criminal activity. Member States also need to introduce verification mechanisms to ensure the beneficial ownership information is accurate. 5MLD will reduce the threshold at which beneficial ownership needs to be identified to 10% for certain types of high-risk entities, as well as bringing trusts under the remit of the regulation.

While beneficial ownership registries offer some support to regulated firms, they are currently at different stages of implementation. So for additional peace of mind, many firms are opting to conduct further

verification against other sources. It's a big job, because to fully map out and verify ownership structure involves looking across a range of data: registered business name, number and address; details of the board of directors and senior persons responsible for operations; the law to which the business is subject; legal owners; beneficial owners; and articles of association.

To get this information means tapping into many different sources: customers; corporate registries and regulators' listings; and supplementary information to fill in gaps or verify source documents from premium data providers.

So whether you are onboarding new customers or remediating KYC for existing customers, the enhanced requirements around beneficial ownership are proving to be a significant challenge for most firms. It is a largely manual and very time-consuming process to gather the necessary information (often from multiple sources, both free and premium), piece it together and map out a visual representation of a company's structure.

MLR 2017 states*:

Where the customer is beneficially owned by another person, the relevant person must –

(a) identify the beneficial owner;

(b) take reasonable measures to verify the identity of the beneficial owner so that the relevant person is satisfied that it knows who the beneficial owner is; and

(c) if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement.

**The UK's 2017 Money Laundering Regulations transpose 4MLD into UK law.*

Reduced simplified due diligence thresholds

Customer Due Diligence (CDD), an essential part of any AML programme, involves gathering relevant information about a customer in order to assess the potential risks to which they expose a firm. Previous AML regulation included the concept of automatic Simplified Due Diligence (SDD). This could be applied when a firm had reasonable grounds to believe a customer fell into certain categories that would automatically classify them as presenting a low risk. 4MLD does away with automatic SDD, requiring all customers to go through a robust risk assessment, which again increases pressure on compliance teams. In essence, it further extends the application of the risk-based approach to the CDD process.

5MLD – Key Changes

Proposed in 2016, the EU's 5th Money Laundering Directive reinforces the changes brought about by 4MLD. It aims to increase transparency about who owns companies and trusts, strengthen legislation around cryptocurrencies and pre-payment cards, clamp down on "high risk" countries and strengthen Financial Intelligence Units.

Transparency

5MLD will make enhanced access to data available to relevant persons as well as to national Financial Intelligence Units. If a trust is a beneficial owner, access will be given following a written request.

Prepaid cards and virtual currencies

Under 5MLD requirements, the anonymous use of prepaid cards will only be permitted for retail transactions below EUR 150 and online transactions below EUR 50. The legislation will extend to cover all entities that hold, store, and transfer virtual currencies, as well as those that provide similar services to auditors, accountants or tax advisors already subject to 4MLD.

Controls for third countries

5MLD also looks to clamp down on the use of high-risk third countries where money laundering legislation is deemed to be too lax or inefficient. The European Commission has earmarked these countries and will put in place systematic enhanced controls for transactions into and out of these countries to hinder flows of illicit funds.

Stronger Financial Intelligence Units

Finally, the role of Financial Intelligence Units (national agencies set up to receive, analyse and disseminate information to combat money laundering) will be strengthened. 5MLD will give them more access to information via centralised bank and payment account registers or data retrieval systems and allow them to cooperate and collaborate more easily. With terrorists and money launderers able to move their funds at speed across borders, reaction time is critical. These changes will allow institutions to react accordingly.

Updated Guidelines for the UK Legal Sector

In March 2018, the SRA released the results of its thematic review, 'Preventing Money Laundering and Financing of Terrorism'. The review highlights the vital role of the legal profession in addressing the issue of money laundering and comes ahead of the Financial Action Task Force (FATF) peer review of the UK scheduled for spring 2018. Following a 2013 report from FATF that concluded that law firms were highly attractive targets for those wishing to launder money, the legal sector is expected to come under further scrutiny during this visit.

Overall, the SRA thematic review found that the majority of firms were "taking appropriate steps to understand and reduce the risk of money laundering, and to comply with the new regulations". However, areas of concern included a lack of record-keeping about how decisions were reached, and slow progress in putting firm-wide risk assessments in place, a requirement under MLR 2017.

Following the SRA's thematic review, The Law Society has published guidelines issued by the Legal Sector Affinity Group (LSAG) to support members in fully meeting regulatory requirements, including the areas raised as a concern in the review.

Balancing Regulatory Obligations with Client and Business Expectations

The challenges of 4MLD have already impacted on business efficiency and customer expectations at regulated firms, who first found that they had to hire compliance staff in huge numbers. At one point, the hiring of large KYC teams was seen almost as a badge of honour. But throwing manpower at the problem had obvious cost implications, so firms are now welcoming technologies that can perform the same tasks with far fewer people.

Internal processes

The regulation also highlighted the need for regulated firms to update their processes. Using people to undertake all CDD work has proved particularly problematic. Reconciling accounts means manually searching databases for relevant information, collating it onto spreadsheets and then analysing it. And using human operators

to undertake manual onboarding is particularly time-consuming, meaning long waits for customers who want to open new accounts. A recent report from Thomson Reuters found it took an average of four interactions with a bank before an account could be opened.[4] Customers may just walk away to a competitor if the process takes too long. Also, if different human operators use different processes, KYC are checks also prone to error, exposing firms to regulatory scrutiny and the risk of laundering illicit money.

Time to revenue

For compliance to be effective, it must not be seen as a stumbling block. Long onboarding times are frustrating for fee-earners or relationship managers, and there is risk that the proper processes will be circumvented in order to bring a customer onboard more quickly, so that revenue can be recognised as early on in the relationship as possible. However, this presents a two-fold risk: potentially onboarding a 'bad actor' with illicit funds; and attracting the attention of the regulator. Already in 2018, we have seen a number of sanctions and some very significant fines taken out against regulated firms.

There is an added benefit to conducting the proper KYC checks up front. Firms will naturally look to cross-sell to their customers across different service areas once KYC checks have been successfully carried out. If customers are rigorously onboarded before their application has been accepted, different service areas can sell in their products straight away, improving efficiency and service, and reducing time to revenue.

Implementing a Best-Practice AML/KYC Process

Every organisation has a different risk profile, so no two AML/KYC programmes are the same. However, there are four key areas that mark out a best-practice process:

1. Quality

Without a complete and accurate picture of a customer's risk profile, it's impossible to make a safe decision about whether they are someone you would want to onboard or continue to do business with. However in many cases, a lack of resources, combined with pressure from the business, will lead to decisions being based on incomplete, poor-quality profiles. This is due to the amount of time it takes to gather the data needed to visualise a customer's corporate hierarchy and beneficial ownership structure. Done manually, the process can take hours or even days: but without this solid foundation, there is no way to comprehensively identify, assess and mitigate regulatory risk.

2. The use of structured data

While new technologies allow for more dynamic monitoring of unstructured, open-source intelligence, structured risk data is still central to screening. Although many global regulatory lists are provided in a structured manner that allows for automation, many still require a combination of technology and manual effort to consolidate and present to the user coherently. And for Politically Exposed Person (PEP) and adverse media data, it is crucial to be able to rely on the baseline definitions of structured databases to focus energies on the right people and the relevant stories. Simply crawling every political exposure and negative media mention will bring a huge number of false positives.

3. Automation

To contain costs and ensure effectiveness, firms must automate and bring scalability to their KYC process. Outside of financial services, the individuals responsible for conducting KYC are often not experts. But regardless of who operates the process, firms need systems that reduce the cost of errors, supervisory overheads, and re-working, while ensuring they are regulator-ready.

Technology, specifically robotic process automation (RPA), has a central role to play in quickly and easily pulling together a single, complete and accurate picture of the customer from all relevant data sources. RPA can precisely replicate the steps a human would perform when accessing data sources, analysing the data and making decisions about whether further checks are needed. It condenses hours of work into minutes.

4. Training

A key success factor in the effective adoption and implementation of a KYC programme is to ensure that training of all relevant staff is specific to their business, and builds awareness and understanding of their regulatory obligations and the broader implications for customer due diligence and its importance. Training also needs to be a regular, auditable and firm-wide. Training and culture go hand-in-hand. The 'tone from the top' must resonate throughout the organisation in order to permeate through to the most junior members, creating a 'buzz at the bottom'.

Delivery of training by experts in AML/KYC is fundamental and should not be left to 'enthusiastic' amateurs as it usually results in courses which are too generic, superficial and poor of quality, which instantly creates barriers to change or skepticism from end users; ultimately having the effect of weakening the programme's importance and effectiveness.

Conclusion

With the introduction of 4MLD and the imminent arrival of 5MLD, the compliance landscape for regulated firms has changed beyond all recognition. The intensified focus on preventing money laundering for criminality and terrorist financing has led to a step-change in the way that regulated firms work with customers. And data leaks such as the Panama and Paradise Papers have highlighted how firms use corporate structures to anonymise their owners.

Before 4MLD, Simplified Due Diligence, with its limited screening requirement, had been the fallback position for most firms' customer onboarding. However the risk-based approach mandated by the new regulation means each customer has to be onboarded depending on their risk profile. In many cases, Enhanced Due Diligence is also needed, and in this instance the LSAG guidance suggests considering whether it is appropriate to:

- seek further verification of the client or beneficial owner's identity from independent reliable sources;
- obtain more detail on the ownership and control structure and financial situation of the client;
- request further information on the purpose of the retainer or the source of the funds; and/or
- conduct enhanced ongoing monitoring.

This toughening regulatory climate also exposes the inefficiencies of manual KYC checking. It's a people-intensive and error-prone process that becomes even more time-consuming and expensive when it must also cover data on UBOs, PEPs, sanctions and adverse media. The threat to customer experience and increased time to revenue is clear, especially when regulation is likely to continue to become more rigorous over time.

For human operators, one of the toughest challenges is to understand corporate hierarchies and UBOs. This needs multiple data sources and can involve information being copied and pasted into spreadsheets for analysis, which is time-consuming and error-

prone. The good news is that technologies can now not only do this in seconds, they can also simultaneously generate an audit trail.

Using technology has four distinct advantages:

- Speed. Information is compiled much more quickly so accounts can be opened faster.
- Understanding. For complex accounts, software can use multiple data sources seamlessly and map out a visual representation of accounts and UBOs.
- Reduced risk. Using technology during onboarding limits the risk of infringing compliance legislation.
- Consistency. Checking all accounts in line with internal policies and procedures avoids the risk of human operators using their own preferred methods or processes for customer onboarding.

The good news for regulated firms is that technology can now automate all but the most complex cases, running thousands of searches to the same compliance policy at a fraction of the cost of manual processing, while improving protection from regulatory risk.

Staff training and awareness throughout the organisation can be the linchpin that determines ongoing success and complete firm-wide buy-in and adoption. So when it comes to selecting a training partner, it's not who you know, but rather what they know; and the deeper their experience and expertise, the better.

C6 and Encompass – The Full KYC Picture, Fast

C6's highly structured and well-defined sanctions, PEP and adverse media content can quickly and efficiently highlight the risks that matter. Combined with KYC automation from Encompass, it can give you the full picture, fast.

Encompass is the only provider of simultaneous, real-time access to multiple sources of global company, registry and person data. Its products robotically search structured and unstructured information sources to automate KYC, AML and EDD policies. UBOs and PEPs are all identified, visualised and verified in seconds. And because the process is entirely automated, Encompass ensures that the same policy is executed to the same criteria on every occasion.

The combination of C6 data and Encompass technology also makes it possible to achieve the understanding of corporate hierarchies that 4AML and 5AML demand. Encompass creates an easy-to-understand visual representation of a company that can be viewed alongside adverse media and PEP records for a full picture.

For financial crime professionals, this blend of structured content and robust technology offers an ideal way to optimise compliance workflows.

Endnotes

1. http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file.
2. https://services.parliament.uk/bills/2016-17/criminalfinances.html.
3. https://flagitup.campaign.gov.uk/.
4. http://www.bobsguide.com/guide/news/2017/Nov/10/kyc-pain-financial-institutions-and-their-clients-are-still-struggling-with-ongoing-challenges/.

Wayne Johnson
Encompass
Level 3, 39 St Vincent Place
Glasgow, G1 2ER
UK

Tel: +44 333 772 0002
Email: info@encompasscorporation.com
URL: www.encompasscorporation.com

In 2012, Wayne Johnson co-founded Encompass corporation, a SaaS business driven by the belief that the best decisions are made when people understand the full picture. As CEO of Encompass, Wayne has lead the creation of the company's Know Your Customer (KYC) automation software for the banking, finance, legal and accountancy sectors.

Wayne has won recognition as an entrepreneur and leader in the information industry. He has raised venture capital in the USA and won multi-million dollar grants from the government. Prior to Encompass, Wayne founded Software Associates in 1986 and served as CEO and chairman until the company was acquired by QHA, a Hong Kong listed Company in 2001. He grew the company to 60 staff with offices in the US and Hong Kong, During this time they built and deployed major applications including telecommunications billing, Internet banking and corporate-wide customer care for the region, major banks, insurers and telecommunications companies.

Joel Lange
C6 an Acuris Company
10 Queen Street place
London, EC4R 1BE
United Kingdom

Tel: +44 203 741 1200
Email: JL@acuris.com
URL: www.c6-intelligence.com

Joel Lange joins us from Dow Jones's Risk & Compliance division where he led the business for over four years through a period of significant growth with a product portfolio focusing on Anti-Money Laundering, Anti-Corruption and Sanctions Compliance. Joel has over a decade of experience in the compliance and transaction operations industry holding senior sales, product and professional service roles at Dow Jones, Accuity and Broadridge. Joel is a regular speaker on compliance topics at conferences around the world. Mr. Lange holds a BA in International Relations from the University of Minnesota and a MSC in International Finance from the University of Westminster.

encompass
the full picture. fast

C6
An Acuris company

Encompass corporation develops technology to automate Know Your Customer (KYC) policies and ensure adherence to Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations in financial, legal and accounting businesses.

With Encompass' market leading technology, KYC checks and onboarding processes can be completed more than 10 times faster and with far lower costs and error rates than manual processes through the use of webbased technology, providing a full audit trail and removing the risk of human oversight.

Founded in Australia in 2012, Encompass launched in the UK in 2015 and now employs more than 50 staff, including more than 30 staff in the UK. It uses real time data from over 30 information providers. Encompass serves more than 200 firms who rely on its products to automate and manage AML/CTF risk and compliance while enabling growth through informed and timely business decisions.

***

Since 2004 C6, an Acuris company, has provided unique, actionable data which helps businesses worldwide manage risk. We are a trusted and independent provider of data intelligence for anti-money laundering, anti-corruption and cybersecurity professionals. Offering a powerful overview and enhanced risk management – our unique database exceeds all expectations and has the most comprehensive database of actionable intelligence relating to Politically Exposed Persons (Pep's) and sanctioned individuals, companies and jurisdictions.

During this time C6 has identified the most relevant local and global sources allowing us to create a unique process of gathering timely, accurate and relevant adverse media relating to the FATF predicated crimes list.

C6 combines human intelligence and code to pinpoint any risks associated with forming new business relationships and a database covers over 200 jurisdiction and over 40 languages. Our suite of KYC search and monitoring data solutions, which access our unique and expanding database, provides you with an accurate risk intelligence data results and a reduced false positives.

Argentina

Justo Lo Prete

Florencia Maciel

Durrieu Abogados S.C.

1 The Crime of Money Laundering and Criminal Enforcement

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

Federal prosecutors in criminal matters are entitled to investigate money laundering. The Office of the General Attorney has an independent organisation as has been established by the Argentine Constitution, and it is entitled to prosecute all crimes. In this sense, it is important to mention that Argentina has a federal political system. Federal jurisdiction and state jurisdiction (provinces) coexist.

There is also an Economic Crimes and Money Laundering Prosecution's Office – "PROCELAC" – that can provide assistance to any federal prosecution.

Additionally, the local Financial Information Unit (FIU) – "UIF" – is the authority *par excellence* in money laundering prosecution.

Finally, the Federal Criminal Procedural Code allows aggrieved individuals to act as private prosecutors if they demonstrate a direct damage caused by the illicit fact.

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 federal offence according to Sections 303 – 306 of the Argentine Criminal Code (ACC). This offence was first introduced in 2001 by Law No. 25,246 about Anti-Money Laundering / Countering Financing of Terrorism (AML/CFT Law), and then amended by several acts in 2011, mainly by Law No. 26,683.

According to ACC Section 303.1, any person who converts, transfers, manages, sells, charges, disguises or in any other way puts in the market, goods amounting to more than Argentine Pesos (ARS) 300,000, originated in a previous illicit act, with the possible consequence that those goods will acquire a licit appearance, shall be punished with prison from three to ten years and a fine. Meanwhile, according to ACC Section 303.4, the same assumption will be considered "minor" money laundering (prison from six months to three years) if the amount of involved goods is less than ARS 300,000.

According to the Argentine Constitution, the burden of proof is on the accuser. The law also establishes that in order to prove money laundering, a predicate "illicit act" must be demonstrated. That means the government has to determine the existence of a previous illicit fact that has resulted in the acquisition of assets or money. This is enough if it meets the *probable* cause standard, which means that no final ruling or sentence is required to prove the predicate offence. "Self-laundering" is punishable in Argentina.

In addition, it is required to prove the *mens rea* of the perpetrator of money laundering. In this sense, the person responsible could only act purposely or knowingly.

Any type of crime could be included as a predicate offence, even tax evasion. The predicate offence shall have an "economic benefit" to be considered "minor" money laundering at least.

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

Argentine AML/FTC Law is only applicable within the local territory. Nevertheless, it is possible to investigate money laundering if the predicate offence took place abroad. The dual criminality principle is required for a crime committed in an extraterritorial jurisdiction.

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

The investigation and prosecution of money laundering criminal offences are assigned to the Argentine Justice system (Courts in Federal Criminal Matters). Every investigation needs first to have the approval of a Federal prosecutor.

On the other side, the UIF's purpose is to prevent, detect and apply sanctions to money laundering cases; the UIF could independently file a criminal complaint for money laundering before the Federal Justice Courts and even promote the investigation to a private prosecutor. The UIF is connected to the Ministry of Finance and is part of the Executive Branch.

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

Corporate liability for money laundering is included in ACC Section 304. In general terms, there is entity liability when a company's representative commits a crime acting under the scope of their authority. Specifically, ACC Section 304 establishes that when the offence has been committed in the name of an entity or with the intervention or to the benefit of an entity, such entity may be subject to sanctions.

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

In case of natural persons, money laundering is punishable by 3 to 10 years in prison and also with a fine. Such a fine could be between 1 and 10 times the amount involved in the relevant money-laundering. The scale previously mentioned shall be increased by a third or reduced to half of its minimum amount if: the perpetrator performs the act habitually or as part of an illicit association or group formed with the purpose to commit these type of crimes; or the perpetrator is a public officer (who also shall be disqualified from public office for 3 to 10 years).

Regarding legal entities, several types of penalties could be applied. The main one is the fine from one to ten times the "undue" benefit that was obtained or that could have been obtained through the actions incurred in breach of this regulation. Other applicable penalties are: the full or partial suspension of the company's activity; the suspension of previously earned government/tax benefits; and the debarment from participating in government biddings and tenders. In certain severe cases, the courts may order that the legal entity must be terminated or cancelled.

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

The maximum period of time to investigate a money laundering case is 10 years (reduced to three years in "minor" money laundering cases). Said term shall be interrupted or suspended under certain circumstances (Section 67, ACC).

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

Money laundering is considered a federal offence throughout the Argentine territory. It is regulated as a crime against the "economic and financial order". It is placed under Section 303, ACC; and no other provincial criminal offence could be introduced in this sense, or in a parallel state jurisdiction.

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?

An asset freezing order issued by the UIF is exclusive to terrorism financing; it can be applied up to a period of six months. An "embargo" is another precautionary measure, which must be ordered by a judicial authority according to Section 23, ACC. The "embargo" tries to maintain the integrity of the assets. Confiscation and annulment of ownership are the hardest measures that can be taken within a criminal investigation and only a judge can decide on those. Confiscation may be ruled for money laundering cases, in Section 305, ACC. In these particular cases, assets could be confiscated without the existence of a criminal conviction and if other requirements convey.

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 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?

The procedure for settling certain crimes is laid out in "suspension of trial" (Section 76 *bis*, ACC), complete damage compensation (Section 59.6, ACC) and also in a section on plea bargain agreements (Section 431 *bis*, Criminal Procedure Code). Suspension of the trial is not applicable due to the penalty scale of the crime of money laundering, and Section 59.6 has only just been added to the ACC. If the penalty for a particular case would not exceed six years of imprisonment, the defendant can plead guilty and apply for plea bargaining. A plea bargaining agreement shall be homologated by the Courts, thus such settlements are 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.

UIF is the administrative authority responsible for imposing money laundering requirements on financial institutions and other businesses. Nowadays there are plenty of anti-money laundering requirements in force, depending on what activity or business is being regulated. In general, every financial institution and business has: 1) a "no-tipping off" obligation; 2) to fulfil the "*know your client*" policy (KYC); and 3) to comply with formal obligations before the UIF, mainly the obligation to report any suspicious transaction, activity or events.

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

To date, there are no other anti-money laundering requirements imposed by self-regulatory organisations or professional associations.

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

Self-regulatory organisations and professional associations are not responsible for anti-money laundering compliance and enforcement against their members. Such members directly assume responsibility or liability before the UIF in case of failure to comply with the AML regime.

2.4 Are there requirements only at the national level?

The UIF's acts, regulations and decrees are enforceable throughout the Argentinean territory and therefore the legal requirements regarding anti-money laundering policy are applicable at national level.

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

The UIF is the competent authority for the examination and enforcement of anti-money laundering requirements. If a fine or sanction is applied, the criteria for examination would be publicly available. The UIF's investigations are confidential but the motivation behind an administrative sanction can be checked on the official site of the UIF.

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 UIF was created in 2000. Among its faculties and duties, the UIF is responsible 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?

Regarding enforcement actions in the administrative law field, sanctions and investigations on the breach of the financial information regime has a statute of limitations term of five years. The statute of limitations for criminal law actions is detailed in 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?

In case of money laundering connected with financing terrorism, the legal entity obligated to fulfil the requirements could be subject to a fine from five to 20 times the value of the assets obtained from the crime, if the legal entity has acted knowingly. The scale is from 20% to 60% of the value of the assets obtained from the crime if the failure was committed recklessly or negligently.

The duty of financial confidentiality must be unconditionally preserved, except if a judge's order deems otherwise. Breaching this duty under other circumstances is punishable with prison and with a fine from ARS 50,000 to ARS 500,000. Finally, any failure related to the financial information regime is punishable with a fine from one to times the total amount of assets or the total transaction amount related to the infraction, if it does not imply a more severe infraction or crime. If the total amount or the value of assets could not be quantified, the scale of the fine will be between ARS 10,000 and ARS 100,000.

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

There are criminal law penalties that include prison, fines and specific sanctions when legal entities are involved (as described in question 1.5). The administrative sanctions are fines and monetary penalties.

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

Most of the violations of the anti-money laundering regime are subject to administrative sanctions. Nevertheless, Section 22 of the AML/CFT Law punishes the breach of confidentiality duty committed by a public officer or employee of the UIF, or by any other member or entity included as an "obliged subject" (the penalty for such breach is imprisonment for between six months and three years). Such punishment would be applied if any confidential information is revealed outside the sphere of the UIF.

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 UIF is responsible for evaluating any infraction of the anti-money laundering regime and imposing the corresponding fine. The administrative process consists on a written proceeding (detailed communication of the accused infraction, the defendant's deposition, production of evidence, closing arguments). The final ruling of the UIF can be challenged at the Court of Appeals on Federal Administrative Matters. Every process is confidential but the final decision regarding the administrative sanctions is public. Several financial institutions have challenged the UIF's decisions in administrative courts of appeal.

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 Section 20 of the AML/CFT Law, there are certain activities and groups of professionals that are considered "obliged subjects" before the UIF. Such obliged subjects must report to UIF any suspicious activity or transaction from their clients, regardless of the amount, that could be related to money laundering or terrorism financing. They also have to obtain from their clients the information and documentation indicated in the resolutions applicable to each category or business, to maintain the confidentiality about their clients' information and compliance with the UIF's regime.

There are 23 categories of "obliged subjects". The categories are as follows: 1) banks and financial institutions; 2) exchange houses or individuals authorised to operate in foreign currency; 3) persons or legal entities whose activity or purpose is gambling, such as casinos; 4) stock agents, managing entities of investments funds, agents of the markets and any intermediaries in the purchase, rent or lending of securities; 5) brokers registered in the futures and options markets; 6) public registries of commerce, agencies of control of legal entities, real estate property registries, property registries of vehicles, pledge registries, boat ownership registries and aircraft registries; 7) individuals or legal entities dedicated to the trading of art pieces, antiques or other luxury objects, stamps or coin investments, or to the export, import, manufacturing or industrialisation of jewellery or objects with precious metals or stones; 8) insurance companies; 9) companies that issue travellers' cheques and entities that operate with credit or purchase cards; 10) companies which transport cash services; 11) postal service companies if they perform wire transfers or transport of money; 12) public notaries; 13) capitalisation or savings entities; 14) customs brokers; 15) the Argentine Central Bank, the Federal Administration of Public Revenues (AFIP), the Argentine Superintendence of Insurance, the Securities Exchange Commission, the General Inspection of Justice, the National Institute for Associations and Social Economy, and the Argentine Antitrust Court; 16) insurance producers, consultants, agents, brokers, assessors and loss adjusters; 17) licensed professionals whose activities are regulated by professional councils of economic sciences; 18) legal entities that receive donations or contributions from third parties; 19) licensed real estate agents or brokers and entities whose corporate purpose is real estate brokerage; 20) mutual and co-operative associations; 21) natural persons or legal entities whose usual activity is the sale or purchase of cars, trucks, motorcycles, buses and microbuses, tractors, agricultural machinery, road machinery, boats, yachts, aeroplanes or aerodynes; 22) individuals or legal entities that act as trustees, and individuals or legal entities that own or are affiliated with trust accounts, trustors and trustees related to trust agreements; and 23) legal entities that organise and regulate professional sports.

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

UIF resolutions state that obliged subjects must follow anti-money laundering proceedings. The said proceedings, outlined in a manual, depend on the nature of the obliged subject's business, but in general terms they consist of appointing a compliance officer, training personnel to identify suspicious transactions, having a confidential register about risk analysis and management of reported suspicious transactions, setting up technological tools to allow for strengthening control and analysis of suspicious transactions, and to perfect policies regarding KYC in order to fulfil the minimum standards required by its own businesses' UIF resolution.

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

Each obliged subject must fulfil a KYC policy, keeping data and documentation regarding their clients. In this sense, they are also forced to analyse the information and documentation provided by their clients and to determine a profile/category for each of them. Keeping a record of the data profile from clients and the documentation of the transactions is mandatory for five years according to the AML/FT, but the UIF's resolutions state ten years.

It is mandatory for banks and financial institutions to identify the individual or legal entity that is carrying on a transaction when it is equal to or greater than ARS 200,000 (or its equivalent in any foreign currency).

Regardless of the involved amount, reporting is required when an obliged subject has detected a suspicious transaction, activity or event. The obliged subject must report this suspicious activity to the UIF within a 150-day period. If the suspicious transaction was related to terrorist financing, the period to report it is 48 hours.

Each obliged subject must analyse, evaluate and explain why the transaction is considered suspicious. They also have to supply to UIF with sufficient information to enable the reconstruction of the transaction. The obliged subjects must submit their report and attached documentation directly to the UIF via an online system called *Reporting System for Suspicious Transactions*.

3.4 Are there any requirements to report routine 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.

Other than "large cash transactions" (the ones equal to or more than ARS 200,000) each obliged subject must file: 1) a monthly report about "international transactions", which must include all funds transfer made in local or foreign currency, between local accounts and foreign accounts; and 2) an "annual systematic report", through which the obliged subject must file information related to its own compliance officer, its own clients' profiles and types, own annual accountable volume, and other corporate and general information about itself.

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

As was mentioned in the previous section, each cross-border transaction must be reported every month by the obliged subjects. It is important to remark that this "monthly report about cross-border transactions" does not constitute a "Suspicious Activity Report" (SAR). Each obliged subject shall then evaluate if the cross-border transaction is suspicious. In that case, the appropriate SAR should be drafted and filed to the UIF. The monthly report about cross-border transactions must contain: the date of the transfer; the amount in ARS or foreign currency; the country of origin of the beneficiary's funds; the identity of the origin and beneficiary's bank; and the individual or legal entities involved in the transfer of funds.

3.6 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?

Due diligence (DD) requirements consists of obtaining and updating data about customers' personal, economical, commercial and tax situation. Since UIF issued the Resolution E-30/2017, in June 2017, there are three types of DDC according to the client's risk-assessment. For low-risk clients, there is a "simplified DD" proceeding, for medium-risk clients there is a "traditional" DD proceeding, and finally high-risk clients have an appropriated enhanced DD proceeding. In general terms, obliged subjects are required to keep updated information about clients' identification, contributing parties, legal status, domicile, main activity, condition

of "politically exposed persons" (PEPs), purpose and functions of their accounts and transactions. Due diligence shall also be enhanced if the client is a foreign or domestic PEP. Financial institutions must request that their clients provide information and sign specific documents (sworn statements) about the origin of the funds involved and the destination or final beneficiary of the funds involved.

3.7 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 the Central Bank of Argentina (known in Spanish as "BCRA"), it is forbidden for foreign shell banks to become shareholders of a financial institution in Argentina. Also, shell banks are not allowed to be shareholders of exchange institutions, or involved in setting up new exchange houses, agencies or offices.

3.8 What is the criteria for reporting suspicious activity?

AML/CFT Law and the UIF's rules consider that suspicious events are those transactions – intended or performed – which raise suspicion with regards to Money Laundering and Financing Terrorism, or which having been previously identified as unusual, after the review and evaluation performed by the obliged subject, do not justify their unusual condition or suspicion still remains that they are linked or are going to be used to launder money or finance terrorism. These transactions must be reported to the UIF through the SAR. The 'unusual transaction' concept is defined as 'those transactions performed or intended in an isolated or reiterated manner, regardless of the amount, which lack economic and/or legal justification, are inconsistent with the client's profile, or which, due to their frequency, regularity, amount, complexity, nature and/or other particularities, do not correspond with the usual market practices and customs'.

3.9 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?

According to Section 14 of the AML/CFT Law, the UIF is entitled to request from any governmental authority (both with federal and local jurisdiction), non-governmental or private entity any kind of information or documentation about legal entities. As a reinforcement of this capacity, before analysis of a report is complete, obliged subjects may not oppose the banking secrecy, tax secrecy, professional secrecy or any type of confidentiality duty in order to avoid the fulfillment of the UIF's request. This faculty allows the UIF access to current and adequate information.

3.10 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 UIF's resolutions rule that payment orders for a funds transfer must be completed with accurate information about the originators and beneficiaries. This information should also be provided to other financial institutions that may be intermediate in the payment.

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

Bearer shares are not permitted in Argentina for any kind of legal entity.

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

As was mentioned in question 3.1, a significant number of non-financial institution businesses are subject to AML requirements since they are obliged subjects before the UIF (Section 20, AML/CFT Law).

3.13 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 was mentioned in question 3.1, customs brokers are subject to AML requirements since they are obliged subjects before the UIF.

4 General

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

There are additional reforms that have been issued by Congress in the last year that – despite not being specifically established for AML – could be useful for enhancing investigations into such crimes. These reforms allow the use of informant agents, revelatory agents or undercover officers for prosecuting certain "complex crimes", where money laundering is thought to be involved.

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?

Argentina has made significant progress during the last years, but despite recent legal reforms, effective implementation of the AML regime continues to be a serious challenge. A clear example is the reduced number of cases that have been successfully prosecuted. This main problem is caused by deficiencies in the judicial procedure, the lack of independence of the judges and prosecutors, and the delays on the investigations. Another obstacle is the lack of interagency coordination between the UIF and the federal security forces or the federal prosecutors.

On the other side, important and necessary measures such as seizure of assets, the freezing of funds, and forfeiting of illicit assets do not have a complete or precise legal framework. Such deficiencies are notable when these measures are applied in real cases. Another relevant defect is that Argentina has still not completed an AML/CFT national risk assessment. Furthermore, it is remarkable that many non-financial business or professionals that are obliged subjects before the UIF, still do not have their own regulatory entities, and the UIF does not have enough resources to adequately supervise them for AML compliance.

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

In 2011, FATF identified structural obstacles and defects in the Argentinean legal system concerning ML/FT. As a result, Argentina was added to the "grey list" (countries which have strategic AML deficiencies). In October 2014, the FATF plenary decided to remove Argentina from the "grey list" and put into effect a careful following of the country, in order to control its continuous concern with every money laundering and financing of terrorism issue identified in the Mutual Evaluation of Argentina follow-up report (June, 2014).

Currently, as a result of 2012's international change of standard, Argentina faces new challenges to fulfil the FATF's 40 recommendations, not only from a technical and formal perspective, but also to display effective implementation. The next evaluation is scheduled for 2022.

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 FATF's official website (www.fatf.org) can provide material in English about Argentina. Also, the CIPCE's (Centre for Research and Prevention of Economic Crime) website (http://www.cipce.org.ar/en) is available in English, but its academic material is in Spanish. The anti-money laundering laws, regulations, administrative decrees and guidance are also in Spanish. In this sense, you can visit the UIF's website (https://www.argentina.gob.ar/uif) and PROCELAC's official site (http://www.mpf.gob.ar/procelac/).

Justo Lo Prete
Durrieu Abogados S.C.
1309 Córdoba Avenue, 6th Floor, Office "B"
City of Buenos Aires (C1055AAD)
Argentina

Tel: +54 11 4811 8008
Email: jlp@durrieu.com.ar
URL: www.durrieu.com.ar

Justo Lo Prete graduated as a lawyer from the Argentine Catholic University School of Law in September 1993. In 1992, Justo joined Durrieu Abogados, and has been the Managing Partner of the firm since 2004. He specialises in general criminal law practices, computer crime, antipiracy and economic criminal law. His expertise is also focused on providing advice to local and foreign banks in compliance, money laundering matters and tax fraud cases.

In 1998 Justo completed a post-graduate course at the University of Belgrano, receiving the official title of "Lawyer specialised in Criminal Law". He also took part in many specialisation courses, among others: the "Oral trial training program" at the Law School of Buenos Aires; the "Practical Business Crime Course" at the Law School of Buenos Aires; and the "Criminal Law Post-Graduate Course" at the Argentine Catholic University.

He speaks Spanish and English.

Florencia Maciel
Durrieu Abogados S.C.
1309 Córdoba Avenue, 6th Floor, Office "B"
City of Buenos Aires (C1055AAD)
Argentina

Tel: +54 11 4811 8008
Email: fmh@durrieu.com.ar
URL: www.durrieu.com.ar

Florencia Maciel graduated with honours from the University of Buenos Aires Law School in July 2016. She is a scholar in the Specialization & Master on Criminal Law at the Universidad Torcuato Di Tella.

She carried out her career's orientation in Criminal Law. Her academic background is also based in criminal litigation techniques training, and she was a member of the team that represented the University of Buenos Aires during the VIII National Championship of Criminal Litigation in 2016. In November 2017, she was rewarded with the first place of the second edition of the "Championship on Criminal Law Litigation". She is a teaching assistant of "Constitutional Guarantees on Criminal Law and Criminal Law Procedure" at the University of Buenos Aires Law School.

Before she joined Durrieu Abogados in August 2016, she worked as a paralegal in the Corporate Law Department of Marval O'Farrell & Mairal (2012–2015).

She speaks Spanish, English and French.

DURRIEU
ABOGADOS

Durrieu Abogados is one of the most prestigious law firms in Argentina, offering a global service in the area of criminal law and economic criminal law.

The firm frequently handles some of the largest and most complex cases, and it has developed its activity both nationally and internationally. The clientele includes individuals, closed held companies and publicly-traded multinational corporations.

Durrieu Abogados also has an extensive network of affiliates, throughout the country and abroad, which enables it to provide comprehensive assistance with legal matters. With more than 25 years' experience in the field of criminal law, the firm has developed different kinds of consulting services, and can handle all types of criminal court cases.

Considering present-day requirements the firm is capable of providing consulting and legal services in Spanish, English, French and Portuguese.

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 A$315,000 fine (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 A$1,575,000 fine (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 the 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 (with the exception of Western Australia) 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 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 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 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 obligations 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 the 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? 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? If so, are the criteria for examination publicly available?

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

AUSTRAC has published a monitoring policy on its website: http://www.austrac.gov.au/about-us/policies/monitoring-policy.

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.

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.

AUSTRAC also has the power to suspend or cancel a remittance provider's registration if they have contravened the AML/CTF Act or present a significant ML/TF risk or people-smuggling 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 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. Only remedial actions 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 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 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.

3.3 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 or e-currency, the RE must report the transaction to AUSTRAC within 10 business days after the day on which the transaction took place.

3.4 Are there any requirements to report routine 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.

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

See the response to question 3.4 above.

3.6 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 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.

3.7 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.

3.8 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 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).

3.9 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.

3.10 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.

3.11 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.

3.12 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).

3.13 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 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?

FATF has 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 (DNFBP), 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, Counsel 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, sanctions and modern slavery. 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 and regularly undertakes independent reviews on behalf of her clients.

In recognition of her achievements, Kate was listed as one of Australia's Best Lawyers for 2015 and 2016 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 solicitor 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, structuring, 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 26 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.

Belgium

Françoise Lefèvre

Rinaldo Saporito

Linklaters

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 BCC 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 term of imprisonment of five years maximum and/or to pay a maximum fine of €800,000. Companies can be sentenced to pay a maximum fine of €960,000.

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 the 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 a serious harm to physical integrity. Some procedural aspects of this provision were deemed unconstitutional by the Belgian Constitutional court and a new law addressing the concerns of the Constitutional Court has been voted but not yet published.

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. The agreement will be rejected if: (i) it has been demonstrated that the suspect's consent to enter the agreement was not free and informed, (ii) the agreement does not correspond to the reality of the facts and to their legal characterisation, or (iii) the sanctions proposed by the prosecution are not proportional 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.

Details of such settlements are not public, only their existence is made available 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.

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 under 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.

Competent Authority	Obliged Entity
Ministry of Economy, SMEs, Middle Class and energy	Companies engaged in lease financing, company service providers, diamond traders and real estate agents.
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 penalty of maximum €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. They essentially ensure that their members respect their obligations of customer and operations 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 the 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? 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?

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?

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 18 September 2017 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 fine of maximum €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 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 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 EEA Member State or in a third country (article 13).

3.3 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).

3.4 Are there any requirements to report routine 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 3.3.

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

See question 3.3.

3.6 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.

3.7 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).

3.8 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 EEA 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.*).

3.9 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.

Current beneficial ownership is not publicly available information in Belgium. However, 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. An implementing decree has yet to be adopted by the government (article 73 *et seq.*).

3.10 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.

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

No, it is not.

3.12 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.

3.13 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?

The draft of the 5th European AML Directive focuses on six main features: (i) designating virtual currency exchange platforms as obliged entities; (ii) setting lower maximum transaction limits for certain pre-paid instruments; (iii) enabling FIUs to request information on money laundering and terrorist financing from any obliged entity; (iv) enabling FIUs and competent authorities to identify holders of bank and payment accounts; (v) harmonising the EU approach towards high-risk third countries; and (vi) improving access to beneficial ownership information.

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, Belgium has taken an approach based on risks in its AML activities and initiatives for many years. Nevertheless, its understanding of these risks is fragmented and incomplete. It appears that the activities exposed to a high risk of money laundering include the diamond trade, in which Antwerp is a leading world centre, and sectors in which cash circulates, such as the trade in used cars and gold. Money transfer services are also particularly exposed to ML risk in this context. The geographic position of Belgium also makes it a target for the transit of illegal movements of funds.

In terms of terrorist financing, the main risks at present concern activities relating to 'jihadists' travelling to countries in the Near and Middle East. Recent events in these regions and the continuing radicalisation in segments of the population create undeniable risk. The money transfer sector is particularly vulnerable to these threats.

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

Belgium was 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 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
rue Brederode, 13
1000 Brussels
Belgium

Tel: +32 2 501 94 15
Email: francoise.lefevre@linklaters.com
URL: www.linklaters.com

Françoise is a specialist in domestic and cross-border litigation, commercial 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
rue Brederode, 13
1000 Brussels
Belgium

Tel: +32 2 501 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 3 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 the 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 9613/98). 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 the 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? 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 3 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 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".

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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, Counsel 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/combate-a-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), 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.

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 intention 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 the 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 the national level?

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.

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

The PBOC is responsible for compliance and enforcement of all AML requirements. In addition, the CBRC, CSRC and CIRC 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? If so, are the criteria for examination publicly available?

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.

Criteria for examination are publicly available as such criteria are set out in various published rules (e.g. the *Guidelines on Establishing AML Monitoring Standards of AML Reporting Entities and the Administrative Measures for Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions*).

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 50,000 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:

- policy banks, commercial banks, municipal credit cooperatives, rural credit cooperatives and rural cooperative banks;
- 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; and
- other non-financial institutions as identified by the PBOC.

The PRC AML law 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 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.

3.3 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.

3.4 Are there any requirements to report routine 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 3.8).

3.5 Are there cross-border transaction 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 3.3 and 3.4. Criteria for reporting cross-border suspicious transactions are outlined in question 3.8.

3.6 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.

3.7 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.

3.8 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.

3.9 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 Industry and Commerce maintains current and adequate institutional information of all corporates established within the PRC. The relevant authorities also publish information of special licences approved by such authorities. The above published information should be sufficient for AML Reporting Entities to meet their AML customer due diligence responsibilities.

3.10 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.

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

The *PRC Company Law* permits joint-stock companies to issue bearer shares.

3.12 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.

3.13 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 PRC AML law regime requires more attention 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?

According to an opinion issued by the General Office of the State Council in August 2017, various AML measures are under consideration (e.g. AML risk monitoring measures of non-financial institutions).

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) (http://www.fatf-gafi.org/countries/a-c/china/documents/follow-upreportthemutualevaluationreportofchina.html), 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.

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

The FATF evaluated the PRC's AML regime in 2011 and the next FATF onsite visit will be around June/July 2018.

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/135153/135173/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 (M)
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 (M)
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

Stéphane Bonifassi

BONIFASSI Avocats

Caroline Goussé

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).

To the exception of petty offences, any offence may constitute a predicate to money laundering, such as tax evasion. On this point precisely, while there is, for prosecuting tax evasion, a prerequisite of a prior notice by Commission on tax offences, there 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 €375,000.00 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 €1,875,000.00 fine, which may equally be raised up to 250% of the value of the property or funds involved in 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 activity, either permanently or for a maximum period of five years.

Money laundering is aggravated under certain circumstances. Penalties for natural persons are upped to ten years of imprisonment and a €750,000.00 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 €3,750,000.00 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 the 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 to 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?

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 employees being convicted for money laundering. However, while banks and other financial institutions have definitely been the target of criminal investigations for money laundering either by the prosecution or an investigative judge, as is evidenced by notable settlements reached between prosecutors and banks, we are not aware of any criminal court convictions of banking or financial institutions, as of yet.

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 one year, 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 €2,800,000.00.

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 open court.

Recently, facing charges of money laundering of tax evasion proceeds, HSBC Private Bank concluded a CJIP with the Special Prosecutor of Financial Crimes, agreeing to a fine and damages for a total of €300,000,000.00.

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 businesses 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 the national level?

To the extent again 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? 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.

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.

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 ten 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 appeals 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 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 programs, 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 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.

3.3 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 here is €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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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 and 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 euros for bureaux de change; 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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.

According to article R. 561-18, a PPE is 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.

Customers that are family members 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?

As far as we know, the implementation in France of additional anti-money laundering measures of the fourth EU Directive against money laundering is under consideration. Among those, additional information regarding the identification of the beneficial owner, to be published by Decree.

There are also discussions at the European Union level on amendments to the fourth EU Directive against money laundering. These amendments would require new financial businesses, including cryptocurrency trading platforms, to abide by AML requirements, provide for an increased cooperation between European Financial Intelligence Units, and greater access to beneficial owner registries.

According to TRACFIN, it would also be under consideration to extend the systematic report obligations for large cash transactions to institutions in the insurance 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?

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 regards 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, Counsel 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 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*.

Stéphane Bonifassi
BONIFASSI Avocats
34 boulevard Haussmann
75009 Paris
France

Tel: +33 1 84 79 41 80
Email: s.bonifassi@bonifassi-avocats.com
URL: https://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 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.

Caroline Goussé
BONIFASSI Avocats
34 boulevard Haussmann
75009 Paris
France

Tel: +33 1 84 79 41 80
Email: c.gousse@bonifassi-avocats.com
URL: https://bonifassi-avocats.com/en

Caroline Goussé is an associate with Bonifassi Avocats, with a focus on white-collar crime. She works on complex financial crime cases involving top management officers and companies in diverse industries, and advises on white-collar crime investigations.

Caroline also works regularly on cases of asset recovery for international clients.

She is licensed as an attorney in both New York and Paris.

Prior to joining Bonifassi Avocats, Caroline was an associate within the corporate litigation team of a French boutique firm, and represented clients in commercial and civil proceedings.

She also has experience working in criminal defence in the United States.

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

Enno Appel

Herbert Smith Freehills Germany LLP

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 on 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 only if committed in a continued manner as part of commercial activity or within an organised association:

- the 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; and offences related to intellectual property, e.g. copyright infringement.

Tax evasion also only qualifies as a predicate offence if committed in a continued manner as part of commercial activity or within an organised association.

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).

Crimes committed abroad are only applicable if: (1) the victim is a German citizen (Section 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 this.

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 the national level? Are there parallel state or provincial criminal offences?

There are no parallel state/provincial offences in Germany and the federal law is enforced by regional state prosecutors.

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?

Directors, officers and employees of financial institutions have been sentenced in Germany in the past years. However, most of these criminal proceedings are resolved without public prosecution and public hearings and only limited information is publicly available.

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 companies trading with goods: 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 the compliance and enforcement.

2.4 Are there requirements only at the national level?

The money laundering requirements are entirely codified in the federal 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? Are the criteria for examination publicly available?

There are no publicly available criteria for the examination of the compliance with anti-money laundering obligations. However, in March 2018 the German regulator BaFin published a consultation document to implement second-level regulations. In this document BaFin gives concrete guidance with respect to the obligations. However, the guidance is not effective yet. 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 of the German Banking Act 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) German Banking Act).

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 trade commercial goods.

3.2 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.

3.3 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 trading commercial 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).

3.4 Are there any requirements to report routine 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 3.5).

3.5 Are there cross-border transaction 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 sale of stocks, derivates 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 obligation 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).

3.6 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 whether the client acts for a beneficial owner and if so, identification of the beneficial owner and verification of the obtained information. (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 have to 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).

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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 trading with commercial 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 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, Counsel 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 link below:

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 online, for example, on the website of the BaFin. There is no English translation of the GWG available as of today.

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 liability lawsuits. One of his key areas of activity is conducting internal investigations, advising clients on anti-money laundering (AML), anti-bribery and corruption (ABC), as well as cases of fraud and embezzlement. Enno is one of the key advisors for an international German bank in the so called "Panama Papers" matter and regularly advises international banks and other clients on regulatory obligations under the anti-money laundering laws, in particular in context of the implementation of the 4th EU Money Laundering Directive (4MLD).

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 in recent years.

Greece

Ilias Anagnostopoulos

ANAGNOSTOPOULOS

Alexandros Tsagkalidis

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 3691/2008 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 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; and
- forming a group or organisation for the purposes of committing one or more of the above-mentioned actions.

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 3 of Law 3691/2008 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 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 the 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 3691/2008 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 3691/2008). 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 the 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 combating 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? 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 3691/2008 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 26 and 31 of Law 3691/2008): 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 51 of Law 3691/2008, 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 in regard to the reporting of suspicious transactions is punishable by imprisonment for three months (minimum) to five years and a fine (article 31 of Law 3691/2008).

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 ten 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 3691/2008 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 €15,000 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 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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 3691/2008 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.

3.7 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 21 of Law 3691/2008 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.

3.8 What is the criteria for reporting suspicious activity?

Please see the answers to questions 3.3 and 3.4.

3.9 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.MI.) which keeps information on all legal forms of businesses in Greece.

3.10 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.

3.11 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.

3.12 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.

3.13 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 3691/2008 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 3691/2008 against money laundering, which was issued following an evaluation by FATF, and the transposition of relative European directives, 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, Counsel 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 the 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 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 an Associate 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 admitted to Bar in 2009 (Athens). 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 Hellenic Criminal Bar Association and the Legal Experts Advisory Panel of Fair Trials International. His practice focuses on money laundering and asset recovery, corrupt practices, tax offences, cybercrime, extradition and mutual assistance. He is fluent in Greek, English and French.

www.linkedin.com/in/tsagkalidis

Hong Kong

King & Wood Mallesons

Urszula McCormack

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 section 25 of the Organized and Serious Offences Ordinance (Cap 455) (**OSCO**). In addition, there is a separate money laundering offence for drug trafficking offences under section 25 of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) (**DTROP**).

The Secretary for Justice, as the head of the Department of Justice (**DOJ**), is the legal body responsible for prosecuting money laundering offences 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?

A person commits a money laundering offence under the OSCO if they "*deal*" with property and that property either wholly or partly represents "*proceeds of an indictable offence*".

"*Dealing*" includes receiving, acquiring, concealing, disguising, disposing, converting, bringing into or removing from Hong Kong or using the property to borrow money.

"*Property*" can include property located in Hong Kong or elsewhere.

In addition to the physical act of *dealing* with property, the relevant person has the requisite knowledge that the property represents criminal proceeds. A person has the requisite knowledge if:

- they have actual knowledge that the proceeds represent criminal proceeds; or
- they have "*reasonable grounds to believe*", that the proceeds represent criminal proceeds. This second limb requires consideration of the person's personal beliefs, perceptions and prejudices, and, if accepted as true, asks whether a reasonable person with the person's personal attributes can objectively be said to have believed that the property represented the proceeds of crime.

For property to represent criminal proceeds it must be derived or realised (directly or indirectly) from payments or rewards received from the commission of an "*indictable offence*" against a law of Hong Kong. Any pecuniary advantage obtained in connection with the commission of that offence is considered a reward.

An *offence* refers to any crime and any contravention or other breach of, or failure to comply with, any provision of any law, for which a penalty is provided. A conviction on *indictment* means a conviction in the Court of First Instance (**CFI**) triable by a jury. Generally, the specific legislation which creates the offence will state that the offence is indictable. For example, the crime of tax evasion is an indictable offence in Hong Kong. Accordingly, tax evasion is a predicate offence for money laundering. Likewise, both public and private sector bribery are indictable offences in Hong Kong and would therefore each be a predicate offence for money laundering.

The elements that need to be proven for money laundering under the DTROP are the same as under the OSCO. Drug trafficking is the predicate offence for money laundering under the DTROP.

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 OSCO and DTROP.

Under section 25 of the OSCO and DTROP, respectively, references to an "*indictable offence*" and "*drug trafficking*" include a reference to conduct which would constitute an offence if it had occurred in Hong Kong, irrespective of where it took place.

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

See the response to question 1.1 above for prosecution authority.

A number of government bodies may investigate and refer money laundering offences to the DOJ, including the Hong Kong Police Force (**Hong Kong Police**), Customs and Excise Department (**C&ED**) and the Independent Commission against Corruption (**ICAC**).

Further, the Joint Financial Intelligence Unit (**JFIU**) is a joint unit staffed by officers from the Hong Kong Police and C&ED who receive, analyse and disseminate disclosures of suspicious transaction reports (**STR**) and other relevant information concerning suspected money laundering.

See the response to question 2.4 for the regulatory authorities.

Other regulatory bodies may have statutory responsibilities that relate to the supervision of anti-money laundering compliance measures, such as the Hong Kong Monetary Authority (**HKMA**) and Securities and Futures Commission (**SFC**).

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

Corporate criminal liability exists in Hong Kong.

Under the Interpretation and General Clauses Ordinance (Cap 1), the term "*person*" in any statute is defined to include any public body and any body of persons, corporate or unincorporated.

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

The maximum penalty applicable to persons convicted upon indictment under the OSCO or DTROP is a fine of HK$5,000,000 and imprisonment for 14 years.

The penalty granted will depend on the value of the property that has been dealt with and the degree of knowledge of the offender.

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

There is no statutory time limit for prosecutions of money laundering offences under the OSCO or DTROP.

In Hong Kong, there are no formal time limits for the commencement of a prosecution for an indictable offence.

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

There are no parallel state or provincial criminal offences in Hong Kong related to money laundering offences.

In relation to Hong Kong's status as a Special Administrative Region of the People's Republic of China, the Basic Law of the Hong Kong was enacted by the National People's Congress in accordance with the Constitution of the People's Republic of China. One of the most prominent features of the Basic Law is the underlying principle of "*one country, two systems*". Under this system, the national laws of Mainland China are not applicable in Hong Kong except for a number of such laws relating to defence and foreign affairs. As such, Mainland Chinese laws on money laundering do not apply in Hong Kong.

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?

A number of different government bodies in Hong Kong have forfeiture and confiscation powers.

Under the OSCO, the DOJ can apply to the CFI for a confiscation order over property belonging to persons convicted of a specified offence (crimes deemed to be organised crime under the OSCO). In order for the CFI to grant the order, the proceeds must be valued at in total at least HK$100,000 and the convicted person must be deemed to have "*benefited*" from the offence. There is no value threshold for a confiscation order against a convicted person under the DTROP.

For some predicate offences that are not deemed to be organised crime under the OSCO, the statute creating the offence includes confiscation orders as a penalty upon conviction. For example, where a person has been convicted of a bribery offence under the Prevention of Bribery Ordinance (Cap 201), then any asset connected with the offence can be confiscated by the courts.

In limited circumstances, property can be confiscated where there has been no criminal conviction. For example, where the ICAC is investigating an allegation of corruption, it may apply to the CFI for a court order to confiscate a person's travel documents and restrain disposal of property, even if that person has not been charged. In addition, the High Court has the power to make freezing orders over a person's assets, where it is satisfied that there is a real risk of dissipation of assets if the order is not made. This process may be used to preserve the asset pool for a limited time, on the understanding that enforcement action may later be rendered.

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

Pursuant to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615) (**AMLO**), banks, other regulated financial institutions and (from 1 March 2018) a range of designated non-financial businesses and professions are under certain obligations to prevent their institutions being used to launder money or finance terrorism. Individuals can also be liable.

Actions have been taken under the AMLO by the HKMA against certain banks and by the SFC against certain licensed corporations. Actions have also been taken against certain money service operators.

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 DOJ may also apply to have the property of the offender seized through a confiscation order (see the response to question 1.10 above).

Criminal trials in Hong Kong are conducted in open court and judgments are generally 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 AMLO imposes legal and supervisory requirements on financial institutions (**FIs**); specifically authorised institutions, stored value facility licensees, licensed corporations, the insurance industry (authorised insurers, appointed insurance agents and authorised insurance brokers), money service operators and the PostMaster General. From 1 March 2018, it also extends to solicitors, accountants, real estate agents and trust and company service providers as "designated non-financial businesses and professions" (**DNFBPs**).

It also provides for the powers of "relevant authorities" and "regulatory bodies" to supervise compliance with those requirements.

In addition, many authorities have issued supplementary guidance under the AMLO to facilitate compliance (**Regulatory Requirements**). While these Regulatory Requirements do not in themselves have the force of law, their evidentiary value in any proceedings under the AMLO give them strong effect in practice.

At a high level, the AMLO requires relevant FIs and DNFBPs to undertake the following, having regard to the risk-based approach:

- conduct customer due diligence and, where applicable, enhanced due diligence on customers before forming a business relationship with that customer;
- identify if any customer is a politically exposed person (**PEP**);
- conduct ongoing monitoring;
- deliver anti-money laundering and counter-terrorist financing (**AML/CTF**) risk awareness training to all staff; and
- maintain records for all transactions for the prescribed time period,

amongst other things.

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

The AMLO is the source of legal anti-money laundering requirements for FIs and DNFBPs.

Some non-FI industries and self-regulatory organisations/professional associations also provided guidance to members on AML/CTF requirements, particularly before the expansion of the AMLO on 1 March 2018. For example:

- the Law Society of Hong Kong issued the "Practice Direction P" to assist its members in fulfilling international obligations on combating money laundering and terrorist financing. Practice Direct P has mandatory requirements on customer due diligence, enhanced/simplified customer due diligence, record keeping, etc.; and
- the Hong Kong Institute of Certified Public Accountants issued the Requirements on Anti-Money Laundering, Counter-Terrorist Financing and Related Matters.

These documents are likely to change in light of the amendments to the AMLO, but the timing is not yet clear. The Licensed Money Lenders Association also publishes guidance for its members of AML/CTF measures. Money lenders are not subject to the AMLO.

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

Generally, yes. Failure to comply in certain instances may result in disciplinary actions and/or call into question the member's fitness and properness in their respective profession. This is in addition to other powers under the AMLO and the DOJ's ability to take action directly for a money laundering offence

2.4 Are there requirements only at the national level?

These requirements only apply at national level. See the response to question 1.9.

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

Relevant authorities and regulatory bodies have various powers to examine compliance with and enforce the requirements.

For example, the HKMA is responsible for examining the compliance of authorised institutions (banks) and stored valued facility licensees. The SFC is responsible for examining the compliance of licensed corporations. The HKMA and SFC can both take disciplinary action against institutions for breaches of the Regulatory Requirements. These powers are in addition to usual police powers of investigation.

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 JFIU is the government body responsible for analysing STRs reported by FIs, DNFBPs, other businesses and the general public. The JFIU's reporting criteria can be found on its website at: https://www.jfiu.gov.hk/en/index.html.

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

There is no statute of limitations for enforcement action by the RAs.

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 provided under the AMLO is a fine of HK$1,000,000 and imprisonment for seven years. This penalty is for conviction upon indictment for an FI, or employee of an FI, who "*knowingly*" and "*with intent to defraud*", contravenes a specified provision of the AMLO. These provisions include the customer due diligence measures, among others.

The maximum penalty for knowingly breaching a specified provision of the AMLO with no intent to defraud, is a fine of HK$1,000,000 and imprisonment for two years.

The penalty regime for DNFBPs is slightly different.

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

The AMLO provides power to the relevant authorities to take disciplinary actions against their respective regulatees.

Specified powers in addition to monetary fines include:

- the power to publicly reprimand; and
- the power to order certain remedial actions, by a date specified by the authority.

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

In addition to civil penalties, the AMLO contains criminal breach provisions in certain cases – for example, an FI may be fined or sentenced to a term of imprisonment if it is found, by the court, to have breached certain specified provisions. See the response to question 2.8.

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?

This depends on the facts. For example, relevant authorities have certain investigative powers to allow them to determine if an FI is complying with the provisions of the AMLO. These powers include the power to enter business premises, make copies of relevant records or documents and to answer questions in relation to certain conduct.

If the relevant authority wishes to pursue a criminal penalty, it must apply to the High Court for an order to that affect. The application for an order, any defence filed and the court's decision are all publicly available.

Otherwise, the authority may choose to take disciplinary action itself. If an FI disagrees with any finding or penalty imposed, then it may be able to apply to the *Anti-Money Laundering and Counter-Terrorist Financing* (*Financial Institutions*) *Review Tribunal* (**Review Tribunal**). The Review Tribunal has jurisdiction to review specified decisions and to hear and determine any question or issue arising out of or in connection with any review. If the Secretary of Justice considers it appropriate to do so, the Secretary may establish additional tribunals for the purposes of any reviews, and the provisions of the AMLO will still apply.

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 AMLO requirements cover:

- companies authorised by the HKMA as "authorized institutions" under the Banking Ordinance (Cap 155);
- companies licensed by the SFC as a "licensed corporation" under the Securities and Futures Ordinance (Cap 571) to carry on a regulated activity (specifically dealing in securities, dealing in futures contracts, leveraged foreign exchange trading, advising on securities, advising on futures contracts, advising on corporate finance, automated trading services, securities margin financing, asset management and credit rating services);
- companies licensed by the C&ED as a "money service operator" under the AMLO to operate a money service such as a money changing service or a remittance service;
- certain bodies authorised under the Insurance Ordinance (Cap 41) (including an insurer, appointed insurance agent and insurance broker);
- the Postmaster General of Hong Kong;
- a person licensed by the HKMA under the Payment Systems and Store Value Facilities Ordinance (Cap 584); and
- from 1 March 2018, each of the DNFBPs.

Subject to certain limited exceptions, the Hong Kong AML/CTF regime focuses on the regulatory status of the particular entity, instead of particular activities to be subject to AML requirements.

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

Yes. The AMLO and Regulatory Requirements require effective systems and controls to prevent and detect ML/TF. Matters which must be specifically addressed in a compliance programme under the AMLO and Regulatory Requirements include customer due diligence, ongoing monitoring, record keeping and staff training.

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

The AMLO prescribes a five-year period for customer relationship and transaction record-keeping. Extreme care is required to ensure that the time periods are carefully reviewed, as they do not generally commence at the time the record is created.

FIs and DNFBPs are not generally subject to large currency transaction reporting, as such. In this respect, the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap 629) is not yet in force – see further, the response to question 3.5.

Notwithstanding, FIs and DNFBPs are under an obligation to continuously monitor their business relationship with their customers. This includes identifying transactions which are unusually large for particular customers (outside a range or pattern of usual customer transaction) and where appropriate, making an STR to the JFIU.

3.4 Are there any requirements to report routine 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 specific requirements to report routine transactions. However, where the requisite knowledge or suspicion arises that property represents the proceeds of an indictable offence, an STR must be made to the JFIU (see the answer to question 3.8).

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

There are no cross-border transaction reporting requirements currently in force in Hong Kong.

The Cross-Boundary Movement of Physical Currency and Nearer Negotiable Instruments Ordinance (Cap 629) has yet to come into operation in Hong Kong. The relevant Bill was approved on 22 June 2017, but the Secretary for Security has yet to publish in a Gazette the date from which the Ordinance will come into operation. Under this Ordinance, individuals will have to disclose when they possess

HK$120,000 or more of physical money or negotiable instruments when entering Hong Kong, subject to certain exemptions, such as passengers in transit. Advance declarations will be required for cargo consignments. The C&ED will be the relevant enforcement agency.

3.6 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?

FIs and DNFBPs must carry out customer due diligence measures in relation to a customer before establishing a business relationship with the customer.

The procedure to be undertaken depends on the customer being onboarded, the associated risk and internal policies and procedures.

In some situations, enhanced customer due diligence may be required, primarily in higher risk situations. Conversely, they may be entitled to conduct simplified due diligence depending on the specific circumstances. The general aim of customer due diligence is to allow FIs and DNFBPs to recognise whether there are grounds for knowledge or suspicion of money laundering or terrorist financing.

The primary requirements include:

- identifying and verifying the customer's identity using reliable, independent source documents, data or information;
- where there is a beneficial owner in relation to the customer, identifying and verifying the beneficial owner's identity, including measures to understand the ownership and control structure of the legal person;
- obtaining information on the purpose and intended nature of the business relationship established with the FI; and
- if a person purports to act on behalf of another customer, identifying the person, taking reasonable measures to verify the person's identity, and verifying their authority to act on behalf of the customer.

Ongoing customer due diligence is also required in accordance with the AMLO.

Where an FI or DNFBP identifies that a customer is higher risk, enhanced due diligence measures should be taken to mitigate this risk. Depending on the nature of the risk identified, examples include obtaining additional information on any connected parties of the customer, obtaining additional information on source of wealth or funds, updating more regularly the customer profile or obtaining approval from senior management to commence the business relationship with the client.

3.7 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 bank must not establish or continue a correspondent banking relationship with a corporation that:

- is incorporated in a place outside Hong Kong;
- is authorised to carry on banking business in that place;
- does not have a physical presence in that place; and
- is not an affiliate of a corporation that: (a) is incorporated in a particular jurisdiction; (b) is authorised to carry on banking business in that jurisdiction; and (c) has a physical presence in that jurisdiction.

In addition, certain Regulatory Requirements indicate the necessary treatment of shell companies, including obtaining satisfactory evidence of the beneficiary owner of any shell company.

3.8 What is the criteria for reporting suspicious activity?

Under the OSCO and DTROP, it is an offence to fail to disclose where a person knows or suspects that property represents the proceeds of an indictable offence or drug trafficking. STRs are also required under other legislation in further scenarios.

Disclosures should be made as soon as is reasonably practical after the suspicion has first been identified.

Examples of the types of transactions where reports should be filed are included in certain Regulatory Requirements and other guidance. They include:

- transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
- transactions, instructions or activities that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
- where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;
- where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
- where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the customer due diligence and/or ongoing monitoring process;
- where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
- the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;
- transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and
- unnecessary routing of funds or other property from or to third parties or through third party accounts.

If an STR obligation arises, there is also an obligation not to disclose to any person any matter which is likely to prejudice any investigation into that matter (that is, "*tipping-off*").

STRs constitute a defence under the OSCO and DTROP for a money laundering offence, but (generally) only if it is made before a relevant dealing and the SFIU consents to that dealing.

3.9 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 Companies Registry (**CR**) maintains information about each Hong Kong company's or registered non-Hong Kong company's directors and direct shareholders.

The CR does not maintain information about the natural persons who are the entities' ultimate beneficial owners. Effectively this means that the CR does not directly assist in compliance with beneficial ownership requirements.

However, new corporate transparency rules took effect on 1 March 2018, meaning that all Hong Kong corporations must maintain a register of their own ultimate beneficial owners, which may be available to the CR and other persons in certain cases.

3.10 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 funds transfers.

Where an FI acts as the *ordering institution* for a wire transfer or remittance transaction equal to or exceeding HK$8,000, the transaction must be accompanied by complete and verified originator information including originator name, number of the originator's account and address or customer identification number or identification document (identification document required for remittance transaction).

The beneficiary institution should record the identity and address of the recipient and verify this information.

Such information should also be included in payment instructions to other FIs. Intermediary institutions are required to ensure that all originator information accompanies the wire transfer.

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

The Hong Kong Companies Ordinance (Cap 622) (**CO**) does not permit ownership of legal entities in the form of bearer shares. However, the CO preserved the status of historical companies formed by bearer shares which preceded the introduction of the prohibition. As such, there are still legal entities in the form of bearer shares in Hong Kong.

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

See the responses to questions 2.1 and 2.2 above in respect of DNFBPs and other self-regulatory organisations and professional associations.

3.13 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 money laundering offences and the suspicious transaction reporting requirements under OSCO and DTROP apply to all persons in Hong Kong and are not business-specific. There are also counter-terrorist financing, sanctions and weapons of mass destruction non-proliferation requirements that also generally apply to all persons in Hong Kong.

The AMLO requirements in respect of FIs and DNFBPs are the only business-specific statutory requirements in respect of AML/CTF compliance (besides more commodities-focused and import/export legislation).

4 General

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

No material reforms proposed at this stage. Many of the reforms regarding DNFBPs and corporate transparency have already been implemented as of 1 March 2018.

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 noted above, a further FATF Mutual Evaluation assessment is expected in 2018 – see the response to question 4.3 below. Relevant details are likely to be identified in the relevant report following that assessment.

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

Yes. FATF evaluated Hong Kong's AML/CTF regime in 2012, releasing its 4th follow up report – mutual evaluation of Hong Kong, China, in October 2012. The report is available on the FATF's website http://www.fatf-gafi.org/media/fatf/documents/reports/Follow%20up%20report%20MER%20Hong%20Kong%20China.pdf.

The next mutual evaluation of Hong Kong is expected to take place in 2018.

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 OSCO and AMLO and related legislation are published on the website: https://www.elegislation.gov.hk/.

The HKMA publishes guidance for authorised institutions and SVF licensees on its website: http://www.hkma.gov.hk.

The SFC publishes guidance on its website: http://www.sfc.hk.

The Insurance Authority publishes guidance on its website: https://www.ia.org.hk.

The C&ED publishes guidance on its website: https://eservices.customs.gov.hk.

Additional information for DNFBPs are published on the websites or their respective regulatory bodies.

The JFIU also makes available various guidance on its website: www.jfiu.gov.hk.

Materials are available in English.

Urszula McCormack
King & Wood Mallesons
13F Gloucester Tower, The Landmark
15 Queen's Road Central, Central
Hong Kong

Tel: +852 3443 1000
Email: urszula.mccormack@hk.kwm.com
URL: www.kwm.com

Urszula McCormack is a financial regulatory specialist based in Hong Kong, focusing on emerging technology and financial crime.

Key areas of her expertise include sovereign digital currencies and blockchain-based tokens, data protection, digital banking, trading and advisory services, peer-to-peer platforms, retail payments and stored value facilities.

In the financial crime arena, Urszula has had a pivotal role in developing the Hong Kong AML/CTF framework, through her work as lead lawyer for The Hong Kong Association of Banks since 2011. Urszula is a Certified Anti-Money Laundering Specialist with ACAMS. She is the author of several publications on anti-bribery and corruption and modern slavery issues, and founded the firm's financial crime, regulatory and investigations blog, *The Laundromat*.

Urszula is Co-Chair of the Policy & Advocacy Committee of the Fintech Association of Hong Kong and is a member of the ASIFMA Fintech Working Group. Urszula is also a member of the Securities and Futures Commission Fintech Advisory Group. Urszula is admitted to practise law in Hong Kong, England & Wales and New South Wales (Australia).

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.

India

Shri Singh

Shri Singh & Chambers of Anuradha Lall

Anuradha Lall

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 ("**Act**") is a national/federal law and has empowered the Directorate of Enforcement (which is a national/federal agency constituted under Section 36 of the Foreign Exchange Management Act, 1999) to prosecute 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?

As per Section 3 of the Act, the government must prove that an individual directly or indirectly attempted to indulge or, knowingly assisted or, knowingly was a party, or was actually involved, in any process or activity connected with proceeds of crime including its concealment, possession, acquisition or use and was projecting or claiming it as untainted property.

The term "proceeds of crime" has a specific definition under Section 2(1)(u) of the Act – being property derived from the commission of a scheduled/predicate offence.

The predicate offences that are listed in the Schedule to the Act *inter alia* include, bribery of public servants, narco-offences, terrorism, securities fraud, customs violations, illegal arms trade, illegal wildlife trade and intellectual property violations. The Schedule has been frequently amended to include a wider ambit of predicate offences. While duty evasion under the Customs Act, 1962 is a predicate offence, at present, only a particular form of cross-border tax evasion is listed as a predicate offence under the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015.

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

There is extraterritorial jurisdiction for the crime of money laundering under the Act.

The Act provides for two possibilities for such jurisdiction. First, if the conduct was at a place outside India and was an offence in that foreign jurisdiction and would also constitute a scheduled/predicate offence under the Act and the proceeds of such conduct were transferred to India. In such a case, money laundering of the proceeds of foreign crimes would be punishable in India. Second, if a scheduled/predicate offence is committed in India and the proceeds of crime are transferred outside India.

The predicate offences with cross-border implications are mentioned in Part C of the Schedule. Chapter IX of the Act provides for reciprocal arrangements with countries with which India has entered into a treaty (or otherwise) for assistance in certain matters, including the procedure for attachment or confiscation of property beyond either country's jurisdiction.

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

The Directorate of Enforcement has been notified as the authority responsible for investigation and prosecution of money laundering criminal offences. The underlying predicate offences, however, are investigated by various agencies including the state police, the Central Bureau of Investigation, the Narcotics Control Bureau, the Directorate of Revenue Intelligence, the National Intelligence Agency and other similar statutory agencies.

In 2005, the Central Government also assigned the Director of the Finance Intelligence Unit ("**FIU-IND**") under the Ministry of Finance of the Government of India as the designated authority to oversee and enforce the anti-money laundering obligations cast on the reporting entities (as explained below).

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

Section 2(1)(s) of the Act expansively defines the term 'person' to include companies and all manner of unincorporated entities which may be held liable under the Act.

Section 70 of the Act provides for corporate criminal liability. The company, and every person who was "in charge of" and "was responsible" for the conduct of the company's business, at the time when the contravention took place, is deemed to be guilty of the contravention. Further, where it is proved that a contravention has taken place due to the negligence of or with the consent or connivance of any director, secretary, manager or other officer of the company, such persons are also deemed to be guilty of the contravention.

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

As per Section 4 of the Act, those found guilty of the offence of money laundering may be punished with rigorous imprisonment ranging from a period of three to seven years, as well as a fine, for all predicate offences except the ones specified under paragraph 2 of Part A of the Schedule (i.e., those relating to narco offences). In case the offence falls into paragraph 2 of Part A, the period of rigorous imprisonment may extend to 10 years.

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

There is no limitation period for money laundering offences. The law of limitation as per Section 468 of the Code of Criminal Procedure, 1973 is applicable to offences punishable with imprisonment for three years or less, whereas the punishment for money laundering offences is for a period of three years or more.

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

Yes, the enforcement is only at national/federal level. There are no parallel state criminal offences under the Act.

It may be mentioned that the Act has not repealed the pre-existing and fragmented statutes/provisions for enforcing conduct that could be classified as 'money laundering'. These statutes include the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act 1976 and the Criminal Law Amendment Ordinance, 1944. While the former is a national/federal statute, the latter provides for limited enforcement by state agencies. This issue has been the subject matter of a recent Law Commission report and a more detailed analysis would be beyond the scope of this Chapter.

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 Directorate of Enforcement has been vested with the power to confiscate any property that is associated with the proceeds of crime while the investigation into the predicate offence is ongoing. This is thus prior to any conviction in either the predicate offence or the offence of money laundering.

Section 5 of the Act allows specified officers of the Directorate of Enforcement to provisionally attach properties (including movable and immovable property) of persons who are believed to be in possession of proceeds of crime. This also applies if such officer believes that the proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation of such proceeds of crime.

Such a provisional attachment order must be sent to a constituted Adjudicating Authority (under Section 8 of the Act) for confirmation. The person whose property has been provisionally attached has a right of hearing at this stage. The orders of the Adjudicating Authority are subject to appeal before a constituted Appellate Tribunal (under Section 25 of the Act). Orders of the Appellate Tribunal are subject to judicial review by the state High Courts and the Supreme Court.

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

A number of investigations are ongoing and trials are pending against the banks in India. However, so far, there have been no reported convictions under the Act.

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 money laundering offences under the Act are not compoundable. They are not subject to either the formal process of plea bargaining under Chapter XXIA of the Code of Criminal Procedure, 1973 or the informal process of an out-of-court settlement.

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 read with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("**Rules, 2005**") imposes anti-money laundering requirements on the "reporting entities". Section 2(1) (wa) of the Act defines a 'reporting entity' to mean a banking company, financial institution, intermediary or a person carrying on a designated business or profession. The terms 'banking company', 'financial institution', 'intermediary' and 'person carrying on a designated business or profession' are each further defined under the Act.

Section 12 of the Act casts certain obligations on these reporting entities to prevent and detect money laundering activities. Every reporting entity is required to:

a) Maintain a record of transactions for a specified period in such a manner as to enable reconstruction of individual transactions.

b) Furnish information to the Director of the FIU-IND relating to certain transactions including *inter alia* cash transactions, suspicious transactions, cross-border wire transfers and counterfeit currency transactions within the prescribed time.

c) Verify the identity of its clients in the prescribed manner.

d) Identify the beneficial owner, if any, of such clients as prescribed.

e) Maintain a record of documents evidencing identity of its clients and beneficial owners, as well as account files and business correspondence relating to its clients for the prescribed period.

Further, the reporting entities are subject to supervision by their respective national regulators. For instance, the Reserve Bank of India ("**RBI**") is responsible for supervision of banks and financial institutions and, the Securities and Exchange Board of India ("**SEBI**") is responsible for regulation of intermediaries in the securities market. The Insurance Regulatory and Development Authority of India ("**IRDA**") is responsible for the regulation of insurers. Under the powers given to them by the Rules 2005, the regulators have issued further anti-money laundering guidelines/

norms/directives to the reporting entities regulated by them in order to enable them to fulfil their obligations under the Act.

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

No. The anti-money laundering requirements for the reporting entities are statutory/regulatory in nature.

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 the national level?

Yes, the anti-money laundering requirements are statutory and regulatory only at the national level.

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

The FIU-IND was set up by the Government of India, under the Ministry of Finance, in November 2004 as the national agency for receiving, processing, analysing and disseminating information relating to cash/suspect financial transactions, cross-border wire transfers and counterfeit currency transactions. The Government of India by notification dated July 1, 2005 appointed the Director of the FIU-IND as the authority exercising exclusive powers *inter alia* under Section 13 of the Act to inquire into and ensure compliance with anti-money laundering requirements by the reporting entities. The Director of the FIU-IND also has powers that are co-extensive with that of the Director of the Directorate of Enforcement.

The information furnished to the Director of the FIU-IND is required to be kept confidential. However, orders passed by the Director of the FIU-IND in cases arising from failure of reporting entities to satisfy their obligations under Section 12 of the Act are publicly available and posted on its website. Where necessary, the Director of the FIU-IND maintains the confidentiality of the accounts and other details in its orders, which are otherwise publicly available.

Further, the orders passed by the regulators including RBI, SEBI and IRDA for non-compliance of the anti-money laundering norms/guidelines/directives issued by them to the reporting entities are also available in the public domain and posted 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?

Yes, as stated above, the FIU-IND is responsible for receiving, processing, analysing and disseminating information relating to suspicious/cash/counterfeit transactions reported by the financial institutions and businesses. The FIU-IND is also responsible for coordinating and strengthening efforts of the national and international intelligence, investigation and enforcement agencies in pursuing global efforts against money laundering and related crimes. The FIU-IND reports directly to the Economic Intelligence Council ("**EIC**") headed by the Finance Minister of the Government of India.

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

The Act prescribes no limitation period for the initiation of proceedings for non-compliance.

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 per Section 13, if the Director of the FIU-IND finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the anti-money laundering requirements under the Act, he may impose a monetary penalty on them which is not less than INR 10,000 but may extend to INR 100,000 for each failure.

A reporting entity or its officers may be subject to these penalty provisions on their failure to satisfy their obligations to maintain records, furnish information to the Director of the FIU-IND or verify the identity of their clients and beneficial owners as mandated under the Act and the Rules, 2005.

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

Under the terms of Section 13(2) of the Act, the Director of the FIU-IND can also:

(a) issue a written warning;

(b) direct the designated director or employees or reporting entity to comply with specific instructions; or

(c) direct them to send reports at prescribed intervals on the measures it is taking.

The Director of the FIU-IND has wide discretion to impose the sanctions and monetary penalties under Section 13(2) of the Act.

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

Yes, the penalties imposed by the Director of the FIU-IND are administrative/civil in nature. However, under Section 63(1) of the Act, any person who is found to have wilfully or maliciously provided false information that leads to arrest or seizure under the Act, is liable for imprisonment for a term which may extend to two years or, a fine which may extend to INR 50,000, or both. However, violations of anti-money laundering obligations that are neither wilful nor malicious can only invite civil sanctions under Section 13 of the Act, as stated 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?

The process for assessment and collection of sanctions is described in Section 13 of the Act. The Director of the FIU-IND is the

prescribed authority for the assessment and collection of data/ records from the reporting entities and upon failure to comply with the requests made, the Director can impose penalties in terms of Section 13. The order of the Director of the FIU-IND is subject to appeal before the Appellate Tribunal under Section 26(2) of the Act.

Yes, the orders of both the Director of the FIU-IND and the Appellate Tribunal are in the public domain and are posted on their respective websites.

Financial institutions have challenged the penalty assessments before the Appellate Tribunal and there are some reported cases.

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 stated above, the reporting entities, i.e., banking companies, financial institutions, intermediaries or persons carrying on designated businesses or professions are subject to anti-money laundering requirements under the Act. Each of these entities is defined under the Act.

'Banking companies' means a banking company or a cooperative bank subject to the Banking Regulation Act, 1949 and includes banks or banking institutions referred to in Section 51 of that Act.

A 'Financial Institution' is a non-banking institution as defined under Section 45(I)(c) 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 the securities market and registered under the SEBI Act, 1992, (ii) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 or any member of such association, (iii) an intermediary registered by the Pension Fund Regulatory and Development Authority, and (iv) a recognised stock exchange under Section 2(f) of the Securities Contracts (Regulation) Act, 1956.

A 'person carrying on designated business or profession' means (i) a person carrying on activities for playing games of chance (including activities associated with a casino), (ii) Registrar or Sub-Registrar appointed under Section 6 of the Registration Act, 1908, (iii) real estate agents, (iv) dealer in precious metals, precious stones and other high value goods, (v) persons engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, and (vi) persons carrying on such other activities as are designated by the government from time to time.

As stated above, these reporting entities are obliged to comply with the obligations imposed under Section 12 of the Act with regard to maintenance of records of transactions, furnishing of information to the Director of the FIU-IND and verifying the identity of their clients and, beneficial owners. Further, these reporting entities also need to comply with the directives and guidelines issued by their respective national regulators like RBI, SEBI, IRDA, etc.

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

Yes, every reporting entity is required to maintain a compliance programme incorporating the guidelines/directives/instructions issued by their respective regulators and the Rules, 2005. For instance, SEBI has issued a 'Master Circular on Anti-Money Laundering ("**AML**") and Combatting Financing of Terrorism ("**CFT**") Obligations' under the Act and Rules 2005 dated December 31, 2010. Similarly, RBI has issued 'Master Direction – Know Your Customer Direction, 2016' which is applicable to all the entities it regulates. The programme is aimed at helping the reporting entities discharge their statutory obligations under the Act and Rules 2005. The elements of the programme therefore typically consist of (i) internal policies, controls and procedures with regard to know-your-client ("**KYC**"), record keeping and reporting of suspicious transactions, (ii) appointment of the designated director and principal compliance officer, (iii) recruitment and training of employees, and (iv) internal audit and control.

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

Under Rule 3 of the Rules, 2005, the reporting entities are obliged to maintain records of all transactions, including those listed below:

i. all cash transactions with a value of more than INR 1,000,000/- or its equivalent in foreign currency;
ii. all series of cash transactions integrally connected to each other which have been individually valued below INR 1,000,000/- or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of INR 1,000,000/- or its equivalent in foreign currency;
iii. all transactions involving receipts by non-profit organisations with a value of more than INR 1,000,000 or its equivalent in foreign currency;
iv. all cash transactions where forged, counterfeit currency notes or bank notes have been used as genuine or, where any forgery of a valuable security or a document has taken place facilitating the transactions;
v. all suspicious transactions;
vi. all cross-border wire transfers with a value of more than INR 500,000/- or its equivalent in foreign currency where either the origin or destination of fund is in India; and
vii. all purchases and sales by any person of immovable property valued at INR 5,000,000/- or more that is registered by the reporting entity, as the case may be.

The reporting entity is required to maintain a record of transactions containing such information as to permit reconstruction of an individual transaction and, in such form, manner and intervals as specified by the reporting entity's regulator. The reporting entity must also develop an internal mechanism for detecting the transactions referred to in the above clauses (i) to (vii) in consonance with the directions/guidelines issued by its regulator.

The Principal Officer of a reporting entity is statutorily obliged to furnish the information relating to the above transactions (except suspicious transactions and the sale and purchase of immoveable property) to the Director of the FIU-IND by the 15th day of each succeeding month. Suspicious transactions must be reported by the Principal Officer promptly to the Director of the FIU-IND within

seven working days of his being satisfied that they are suspicious. With regards to transactions relating to the purchase and sale of immoveable property valued at INR 5,000,000 or more, the same must be reported to the Director of the FIU-IND every quarter by the 15th day of the month succeeding the quarter.

3.4 Are there any requirements to report routine 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, only large cash/suspicious transactions as listed above need to be reported to the Director of the FIU-IND.

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

The cross-border transactions and manner of reporting by the reporting entities is as stated above.

3.6 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 9 of the Rules, 2005, every reporting entity is required to conduct client due diligence:

a) at the time of commencement of an account-based relationship;

b) (i) while carrying out a transaction of an amount of INR 50,000 and above, whether conducted as a single transaction or several transactions that appear to be connected, or (ii) while carrying out any international money transfers; and

c) when there are doubts about the adequacy or veracity of previously obtained client identification or there are suspicions of money laundering or financing of terrorist activities.

Further, the reporting entity must exercise ongoing due diligence with respect to each client and examine the transactions to ensure that they are consistent with its knowledge of the client, his business, risk profile, etc.

Under Rule 9(14) of Rules 2005, the regulators are required to issue client due diligence/KYC guidelines to implement the Rules, 2005 and special or enhanced client due diligence have been specified in guidelines issued by SEBI, RBI and IRDA based on client risk assessment.

Thus, for instance, SEBI's Master Circular on AML/CFT dated December 31, 2010 sets out a non-exhaustive list of 'clients of special category' including trusts, charities, non-governmental organisations, politically exposed persons, high-net-worth clients, companies having close family shareholdings, clients in high risk countries, non-face-to-face clients or clients with a dubious reputation to whom enhanced due diligence must be applied.

3.7 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 RBI's Master Direction – Know Your Customer Direction, 2016 banks have been *inter alia* advised that correspondent relationships shall not be entered into with shell banks and that the correspondent banks shall not permit their accounts to be used by shell banks.

3.8 What is the criteria for reporting suspicious activity?

"Suspicious transaction" as defined in Rule 2(g) of the Rules, 2005 means a transaction, including an attempted transaction made in cash or otherwise, which, to a person acting in good faith:

(a) gives rise to reasonable grounds for suspicion that it may involve the proceeds of a Scheduled offence regardless of the value involved;

(b) appears to be made in circumstances of unusual or unjustifiable complexity;

(c) appears to have no economic rationale or *bona fide* purpose; or

(d) gives rise to reasonable grounds for suspicion that it may involve financing of activities relating to terrorism.

The definition of the term 'transaction' is very wide under the Act and *inter alia* includes the purchase, sale, loan, pledge, gift, opening of an account, deposits, withdrawals, use of safety deposit and entering into a fiduciary relationship.

3.9 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 Government – through the Ministry of Corporate Affairs – maintains a database of all companies, recognised as such under the Companies Act, 2013, including beneficial ownership.

3.10 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, RBI Master Direction – Know Your Customer Direction, 2016 mandates that accurate information about originators must be included in payment orders for a funds transfer. All cross-border wire transfers including transactions using credit or debit cards must be accompanied by accurate and meaningful originator information including the name, address, account number or a unique reference number, as prevalent in the country. Domestic wire transfers of INR 50,000 and above must be accompanied by originator information including the name, address and account number.

However, interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions are exempt from the above requirements.

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

No, the Companies Act, 2013 requires that shares be held in the name of the person/member and bearer shares are not permitted.

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

No, the requirements of reporting for non-financial institutions are the same as specified in Section 12 of the Act above.

3.13 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?

While the Act and Rules, 2005 do not prescribe any anti-money laundering requirements applicable to any specific business sectors or geographical areas, Rule 13 of the Rules 2005 requires each reporting entity to carry out risk assessment to identify, assess and take effective measures to mitigate its anti-money laundering and terrorist financing risk for clients, countries, geographic areas, products, services, transactions or delivery channels, which are consistent with any national risk assessment conducted by the Central Government authority. The regulators have further issued guidelines incorporating the requirements of Rule 13. Thus, RBI Master Direction – Know Your Customer Direction 2016 imposes a general obligation to categorise the clients as low, medium and high risk based on the reporting entity's risk assessment, but the Directive does not specify any sectors or geographical areas, as such. In compliance with the recommendations of Financial Action Task Force ("**FATF**"), the Government agencies embarked on a massive risk assessment exercise in January 2016 to identify the sectors which are susceptible to money laundering and that process is ongoing.

4 General

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

The anti-money laundering laws in India in their present form are relatively recent. The Act has undergone several material amendments in the last nine years and remains subject to frequent amendments. Recently, the Parliament introduced the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 and amended the Benami Transactions Act, 1988. There are also pending amendments to predicate offences, such as the Prevention of Corruption Act, 1988.

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. After becoming a member of the FATF, India was placed in a regular follow up process for mutual evaluation processes. After seven follow up reports, the FATF's 8th follow up report in June 2013 recognised that India had reached a satisfactory level of compliance with all the core and key recommendations of FATF. Consequently, India has been removed from the regular follow up process.

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

Yes. In its bid to become a fully-fledged member of the FATF, a joint FATF/Asia Pacific Group Mutual Evaluation Team visited India in November-December, 2009 for an on-site assessment of India's compliance with the 40+9 Recommendations of the FATF.

The Mutual Evaluation Report on India and India's membership issues were discussed in the third meeting of FATF Plenary-XXI held in Amsterdam, the Netherlands from June 23 – 25, 2010. FATF Plenary adopted the Mutual Evaluation Report on India on June 24, 2010 and on June 25, 2010 India was added as the 34th Country Member of FATF.

Thereafter, India was placed in a regular follow up process for mutual evaluation processes as stated above and, after the FATF's 8th follow up report dated June 2013, India was removed from the regular follow up processes.

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?

Information as stated in this Chapter is freely available on the Internet. Statutes, rules, regulations, etc. are publicly available in the English language at the websites of the FIU-IND and national regulators like RBI, SEBI, etc. However, care must be taken in accessing current versions of these documents, due to frequent changes and amendments.

Shri Singh
C 401, LGF, Defence Colony
New Delhi 110024
India

Tel: +91 11 4185 4045
Email: shrisingh@delaw.in

Shri is a practising criminal lawyer and the head of his chambers in Delhi. His practice focuses on anti-corruption and anti-money laundering trials. He has worked on a number of leading criminal trials including elements of the multi-billion dollar 2G Telecom trial and coal allocation trials. He regularly advises corporations and individuals in navigating multi agency investigations and trials. Shri is an alumni of the prestigious National Law School of India University, Bangalore, 2004.

Anuradha Lall
Chambers of Anuradha Lall
E-6, 1st Floor, Connaught Place
New Delhi 110001
India

Tel: +91 98 1060 9959
Email: anu.lall@lall.in
URL: www.lall.in

Anuradha Lall is a lawyer based in New Delhi whose practice focusses on White Collar Crime and Dispute Resolution. Anuradha has advised globally leading investment banks and multinationals on high-profile investigations in India arising from violation of US FCPA and anti-bribery laws, fraud and compliance issues. Anuradha has represented these clients before the High Court and various tribunals and authorities in a vast range of disputes arising with employees, regulators or third parties. Anuradha has more than 20 years of work experience and prior to setting up her White Collar Crime practice, she worked with top-tier law firms in both India and USA.

Anuradha has been consistently listed as a recognised practitioner in White Collar Crime in India by *Chambers & Partners* (UK).

Anuradha studied at Campus Law Centre, Delhi (1994) and then did her LL.M. from University of Glasgow (1997) and later, a second LL.M. from Case Western Reserve University, Cleveland, USA (2006). Anuradha was a gold-medallist in Delhi University and obtained full scholarships to pursue her studies abroad.

SHRI SINGH

CHAMBERS OF ANURADHA LALL

Isle of Man

Sinead O'Connor

DQ Advocates Limited

Kirsten Middleton

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 Financial 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 (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 the 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.

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 the 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? 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 has to 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 recently used its civil powers for the first time 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.

The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018 has recently received Royal Assent. It provides the GSC with similar powers to the FSA including the ability to levy civil penalties.

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 are '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 & trust service providers, pension providers, money transmission agents, tax advisers, charities, payroll agents and those businesses involved with virtual currency.

3.2 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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 3.3, 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.

3.6 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.

3.7 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.

3.8 What is the criteria for reporting suspicious activity?

Section 142 of POCA creates the failure to disclose 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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 to 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?

The Anti-Money Laundering and Other Financial Crime (Miscellaneous Amendments) Bill 2018 is currently before Tynwald (the Isle of Man's Parliament). The Bill is in response to certain of the findings of the MONEYVAL assessment. There is also the draft Anti-Money Laundering and Countering the Financing of Terrorism (Unregulated Trustees) Code 2017 which is associated with the Bill.

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 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 has recently been submitted.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Counsel 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

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*.

Israel

Dr. Zvi Gabbay

Barnea

Adv. David Gilinsky

1 The Crime of Money Laundering and Criminal Enforcement

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

Section 2 of the Anti-Money Laundering Law 5760-2000 (the "**Law**") defines 'Core Offences' in relation to the Law. These offences carry a sentence of at least 10 years' imprisonment or a fine of twenty times the amount specified in section 61(a)(4) of the Criminal Sentencing Law. The Fight on Terror Law, 5776-2016 (the "**Terror Law**") also contains further provisions.

The requirements are expanded upon in further detail in the Anti Money Laundering Order (identification, reporting, and record keeping obligations of banking corporations to prevent money laundering and the financing of terror) 5761-2001 (the "**Regulations**").

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 prove an offence, the government must establish the guilt of the defendant beyond all reasonable doubt, before the relevant criminal court.

Tax Offences are included in the First Addendum of the law as offences that can be the source of a money laundering offence. Paragraphs 17, 17A, 17B, and 17C all relate to tax (e.g. VAT, income, tax, property tax).

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

Section 2(b) of the Law states that an Offence also includes an offence committed in another state, so long as the act constitutes an offence under the law of that state.

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

Section 12 and 11m of the Law defines the 'Authority'. It includes: The Banking Supervisor; The Chairman of the Israel Securities Authority; The Capital Markets Authority; The Supervisor of the Postal Bank; the Supervisor over Diamond Dealing; and the relevant officer in the Justice Ministry, all according to which entity is being regulated.

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

Section 7 and section 8A(b) detail the corporate entities that are subject to corporate liability under the Law and these are listed in the Third Addendum to the Law.

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

The maximum penalty available depends on the exact nature of the offence. For an offence under section 3 of the Law, the maximum penalty is either a prison sentence of up to ten years, or a fine of up to twenty times the amount specified in section 61(a)(4) of the Criminal Sentencing Law, or both.

For an offence relating to avoiding a report to the authorities, under section 7 or 8A of the Law, the maximum sentence is a prison sentence of up to five years or a fine of up to eight times the amount specified in section 61(a)(4) of the Criminal Sentencing Law, or both.

For an offence relating to the use of Forbidden Property, under section 4 of the Law, the maximum sentence is a prison sentence of up to seven years or a fine of up to 10 times the amount specified in section 61(a)(4) of the Criminal Sentencing Law, or both.

Where the judge gives a sentence lower than the maximum stated in the Law, then he needs to explain in his judgment the reasons for lowering the level of the sentence in the context of the seriousness and the elements of the crime and the perpetrator, under section 35(a) of the Criminal Sentencing Law.

Companies do already have criminal liability under section 23 of the Criminal Sentencing Law, and this can relate to any crime.

There is a White Paper, which was published in October 2014, which proposes an amendment to the existing criminal liability of companies, so as to include an 'obligation of supervision'. This new obligation was specifically intended to cover offences like money laundering. The proposal was to have the breach of the obligation of supervision be a separate, and less serious offence than the actual offence, but one where the burden of proof would be on the company, as there would be an automatic rebuttable presumption that if a person in the company commits an offence, then the company had

breached its obligation of supervision. The amendment was also intended to more clearly define and circumscribe the 'Hierarchical test' and the 'Functional test' which have so far only been laid down in jurisprudence.

The 2014 White Paper has not yet been upgraded to a Bill, nor passed into Law.

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

The offence of money laundering is subject to the Israeli Statute of Limitations, which states in section 5(2) that the limitation period for actions not relating to land is seven years from the date the cause of action arose. However, there are exceptions/clarifications to this rule. For example, if the defendant was abroad, then the limitation period is suspended while he is abroad, and re-starts only when he returns to Israel. Likewise, if it was not possible for the prosecutor to know about the offence, then the limitation period only commences when the prosecutor found out, or should have known about the offence.

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

The State of Israel is a nation state that has no states or provinces which have devolved powers. Therefore, all enforcement is through the national courts.

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 law provides for forfeiture of the criminal assets under section 21 of the Law. This requires the court, except in exceptional circumstances which the court must detail in its judgment, to impose a forfeiture order on a person found guilty of a crime under sections 3 or 4 of the Law, over the property relating to the crime, or property to the value of the property involved in the crime. The court can also impose a forfeiture order over assets held by another person where those assets have been given to the person or paid for by the guilty party.

If the court is of the view that taking forfeiture proceedings as part of the criminal case will impose difficulties on the conduct of the case, then it can order that the forfeiture hearings be done separately in a civil procedure. (Section 21(e).)

Section 22 of the Law permits forfeiture in civil proceedings in the District Court, at the request of the District Prosecutor, where the following two conditions are met:

a) the property has been acquired in the course of a crime under sections 3 or 4 of the Law; and

b) the person who is the suspect in the crime is either not in Israel permanently, or cannot be located, and therefore it is not possible to indict him, or the property only became known after a conviction in the case.

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

Yes, there are numerous instances of directors, officers, and employees being convicted of money laundering. IMPA collects the court judgments and provides them in an easily accessible format on their Hebrew language website. The web address for this page is: www.justice.gov.il/Units/HalbanatHon/MeydaMishpati/Psika/Pages/Verdicts.aspx. Unfortunately, the page is not provided on the English website.

In the Bank Leumi scandal, where the bank and its directors were accused of helping American citizens avoid tax liabilities, the Tel Aviv Commercial Court, with J Kabub sitting on the bench, approved a settlement in the various derivative actions, whereby the senior management involved returned 5 million NIS of bonuses received in previous years.

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?

It is possible, as discussed in the answer to question 1.9, for financial penalties and forfeiture to be used against offenders. IMPA, in its annual report, which is made available on its website, provides an overview of a selection of such cases. Three such cases from the IMPA 2016 Annual Report (pages 58 to 61), include:

1) An inspection by the Finance Ministry of an Insurance company found shortcomings in the adherence to various AML requirements, and in a decision dated 28.09.2016, a fine of 250,000 NIS was imposed.

2) The Currency Supervisor inspected and subsequently fined a bureaux de change business a total of 300,000 NIS for failings in AML procedures.

3) The Tax Authority arrested and subsequently fined an Ethiopian national who was seeking to leave Israel via Ben Gurion airport under the voluntary repatriation scheme of illegal immigrants, and was arrested whilst having US$190,450 of undeclared cash in his bags, and a further US$70,000 elsewhere. He was fined 300,000 NIS.

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.

Section 2 of the Anti-Money Laundering Law 5760-2000 (the "**Law**") defines 'Core Offences' in relation to the Law.

These offences carry a sentence of at least 10 years' imprisonment or a fine of twenty times the amount specified in section 61(a)(4) of the Criminal Sentencing Law. The Fight on Terror Law, 5776-2016 (the "**Terror Law**") also contains further provisions.

The requirements are expanded upon in further detail in the Anti Money Laundering Order (identification, reporting, and record keeping obligations of banking corporations to prevent money laundering and the financing of terror) 5761-2001 (the "**Regulations**").

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

No. The requirement comes from the Law. Please see the response above to question 1.4. Section 11m and section 12 of the Law

provides a list of the major regulatory bodies who are each defined as the 'Authority' for the purpose of AML supervision, oversight, and enforcement in relation to their membership and the organisations they oversee.

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

As per the answer to question 2.2 above, the Law gives the regulatory bodies defined under section 11m the responsibility for ensuring AML compliance and enforcement within their membership body.

2.4 Are there requirements only at the national level?

Yes, there are.

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

Each financial regulator as listed in the list of Authorities in section 12 of the Law, is responsible for compliance and enforcement of the Anti-Money Laundering requirements by the entities under its supervision.

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 Israel Money Laundering and Terror Financing Prohibition Authority (IMPA) (website: http://www.justice.gov.il/En/Units/IMPA/AboutImpa/Pages/default.aspx) was established in 2002 as a financial intelligence unit acting in accordance with the international rules concerned with the combat of money laundering prescribed by the FATF and is overseen in Israel by MONEYVAL. IMPA is an independent Intelligence Authority. As such, IMPA is an administrative unit that does not have investigative powers.

IMPA performs its mission in coordination with the Israel Police (IP), the Israel Security Authority (ISA) and the financial regulators, and assists them in fulfilling their missions and enforcing the AML/CTF regime.

IMPA's main added value is the ability to collect and interpret the financial information contained in its database – which facilitates the detection of suspicious entities who are involved in money laundering or terror financing activities. This function is achieved, *inter alia*, by means of analysing a collection of information from various governmental and financial institutions, as well as information shared with peer Financial Intelligence Units (FIUs) in other countries. IMPA also serves as a centre of research and legal information for money laundering and terror financing, and its employees are considered to be specialists in the collation, analysis and extraction of intelligence from raw data available to IMPA.

Accordingly, IMPA serves as a buffer between the financial sector and the investigative law enforcement authorities. IMPA only disseminates information to law enforcement authorities when it is deemed to be relevant to suspected money laundering or terror financing activities, as prescribed by law.

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

The Limitations Law, 5718-1958, is the applicable statute of limitations.

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?

Whenever a regulatory authority finds that an entity under its supervision has failed to comply with an AML requirement of either identifying customers, or making obligatory reports and disclosures, it may choose to establish a special committee to impose a financial penalty on the regulated entity. It may do this either in parallel to, or instead of, a criminal process, at its discretion.

The maximum level of financial penalty is laid down in the Regulations and is based on the sum specified in section 61(a)(4) of the Criminal Sentencing Law. See the answer to question 1.6 above.

The level of the financial penalty imposed in a particular case will depend on the specific circumstances of the case, and factors such as whether it is a first time offence, or a repeat offence, the financial extent of the offence, the seriousness, whether the defendant co-operates in investigating the offence and its impact, and what if any steps had been taken to seek to prevent an offence occurring, which can all work to reduce, or even eliminate a financial penalty.

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

See the answer to question 1.6 above.

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 and civil. The penalty can also be criminal. There are also financial penalties or fines. The procedure for imposing these is laid out in sections 12 to 20 of the Law. Each Authority has a committee, comprised of three people, which makes decisions on imposing fines. The fine that can be imposed is up to 10 times the amount specified in section 61(a)(4) of the Criminal Sentencing Law, for any breach of sections 7, 7A, 8A, 8B or 11C of the Law.

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 Committees referred to above in the answer to question 2.10 have to send a demand in writing for the payment of the fine once they have decided on a fine. The person being fined has 30 days from the date he receives it to pay the fine. The collection of the fine is governed by the provisions of the Tax Ordinance (Collection). Where a fine is not paid on time, then it attracts interest and is indexed to the CPI. Section 20 of the Law deals with appeals against a fine, which may be lodged at the Magistrates Court within 30 days of receiving the demand for payment. Unless the Committee or the

Court has ordered otherwise, the mere fact of the submission of an appeal does not delay the obligation to pay the fine within 30 days. If the appeal is accepted by the court after the fine has been paid, then the amount of the fine will be refunded with interest and indexation. A decision of the Magistrates court on an appeal against a fine can be appealed to the District court and will be heard by a single judge.

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 and all business providing financial services that are listed in the Third Addendum to the Law are subject to the requirements of the law. These include stock exchange members, trading platforms, portfolio managers, insurers and their agents, provident fund managers, people offering credit and deposits, the Postal Bank, a P2P lending platform, dealers in precious stones, providers of a business service and currency service providers.

The basic obligation imposed is under section 7 of the Law, and requires the entity providing the services to have identified their client, and any beneficiary of their client, all according to the specific requirements of the Regulations, before undertaking any business activity for them. Section 8B extends a similar obligation to anyone else providing a business service relating to the purchase and sale of land, or a company, trust or business, or its assets, which includes entities such as law firms and accountants. They must also submit the ID information they obtain to the database set up by the Justice Ministry under section 28 of the Law.

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

Yes, banks and any other entity regulated by the Bank of Israel, and entities regulated by the Israel Securities Authority, and entities regulated by the Capital Markets Authority, are expected to have an internal policy for combatting money laundering, and to have a programme for ensuring that the policy is being adhered to and that it is properly understood by the employees of the firm.

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

Regulation 8 of the Regulations details the thresholds at which reports must be made by banks on cash transfers into and out of bank accounts. These include:

- any deposit or withdrawal of Israeli or foreign currency exceeding 50,000 NIS;
- any deposit of cash for the purpose of sending funds to a territory listed in the Fourth Addendum, or the withdrawal in cash of any funds received from a Territory in the Fourth Addendum, where the amount exceeds 5,000 NIS;
- any conversion of cash from or to a foreign currency where the amount exceeds 50,000 NIS;
- any Bankers' Cheque in Israeli or Foreign currency where the amount exceeds 200,000 NIS;
- any purchase of travellers' cheques or bearer securities of a foreign financial institution where the amount exceeds 50,000 NIS; where the foreign financial institution is in a territory listed in the Fourth Addendum, then any amount exceeding 5,000 NIS; and
- presentation of cheques drawn on a foreign financial institution where the value of the cheques exceeds 1 million NIS; where the foreign financial institution is in a territory listed in the Fourth Addendum, then where the value of the cheques exceeds 5,000 NIS.

3.4 Are there any requirements to report routine 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.

Regulation 10 provides an exemption for a bank from making a report under Regulation 8 where the entity that has made or received the transfer or withdrawn or deposited the cash is a public institution, another banking institution, the Postal Bank, an insurer, a stock exchange member, a provident fund manager, or a fund.

Section 9 of the Law specifies a requirement to declare cash held by a person upon entering or leaving the State of Israel. The amount is specified in the Fourth Addendum to the Law and currently stands at 50,000 NIS. Where a person enters of leaves Israel by a land border with Gaza or with Jordan or Egypt, the amount is 12,000 NIS.

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

These are specified in the answer to question 3.3 above.

3.6 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 3 of the Regulations specifies the due diligence ID requirements that banks (and other regulations extend this to other financial institutions in Israel) have to comply with when identifying customers. The requirements vary slightly depending upon whether the customer is an Israeli resident or a foreign resident. Article 6 of the Regulations requires the ID, or certification, to be done face to face, meaning in person, in the presence of an employee of the bank, an Israeli lawyer or an Israeli diplomat.

For Israeli residents: The bank must receive the applicant's up-to-date ID document or a certified copy, and must check this against the Population Registry records, to verify the most recent issue date. Equally acceptable as forms of ID for this purpose are a New Immigrant Certificate within 30 days of issue, and an Israeli passport, where the bank believes the person is no longer permanently resident.

For Foreign residents: The bank must receive the applicant's up-to-date passport or laissez-passer or a certified copy, and must compare the details on this document with another official document carrying the applicant's picture and ID number. Where there is no ID number, then the document must carry the name, address, and date of birth of the applicant.

For Israeli corporates: The bank must receive a certified copy of:

- the company's certificate of incorporation;
- the articles of association, and memorandum of association if it exists;
- a lawyer's certification that the Company exists, its name and registered number, or alternatively the bank can verify these facts against the Company Registrar's database;
- the minutes of the relevant board or committee authorising the Company to open the bank account; and
- the list of authorised signatories in the Company for managing the account.

For foreign corporates: The bank must receive the equivalent documents to those required of Israeli companies. Where the document is not available it must receive a lawyer's certificate that the document or the facts do subsist. If the Company is from a jurisdiction where there is no central Companies Register, then the bank must receive a lawyer's certificate to that effect.

There are additional requirements for residents of the administered territories, and for foreign politically exposed persons. The second paragraph of the Fourth Addendum of the Regulations lists countries which are either not FATF compliant, or which are enemy states, and therefore where additional reporting requirements exist in relation to any payments or receipts (see the answer to question 3.3).

3.7 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, they are prohibited. A bank account for a foreign bank is governed by article 5A of the Regulations, and this is defined as a Correspondent bank account. Such accounts may only be opened where all the relevant requirements of article 5A are met, and this includes details of the foreign bank's financial regulator and the anti-money laundering authority. For a non-OECD country bank, an Israeli bank must receive all of the following before it may open a bank account:

- a copy of the authorisation from the bank's home regulator;
- the bank's incorporation documents; and
- either a reference from an OECD bank that already manages a correspondent account for that bank, or some other document that evidences that the bank holds such accounts and is answerable to a regulator and an anti-money laundering authority that requires proper identification of clients.

3.8 What is the criteria for reporting suspicious activity?

Article 9 of the Regulations specifies unusual activity, and the parameter for reporting it. The list of activities that can *prima facie* be deemed unusual is provided in the Second Addendum to the Regulations. Unusual Activity is defined as 'activity which on the basis of the information possessed by the bank raises a suspicion of a connection to illegal activity under the Anti-Money Laundering Law or under the Fight Against Terror Law'.

The information that must be included in the report is listed in Regulation 11.

3.9 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 Registrar maintains a comprehensive register of companies and partnerships in Israel with details of all directors and shareholders, and other relevant information, and this is accessible online.

3.10 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.

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

No. This was made illegal by a change in the Companies Law on 17 March 2016. The provision went into force on 17 September 2016. All relevant provisions of the Companies Law that previously referred to bearer shares have had references to bearer shares removed. Any bearer shares still in existence at that date were either removed or converted to dormant shares. Holders of bearer shares were able to convert them to registered shares before the change in law took effect by presenting them to the Company, and the Company issuing registered shares with identical rights.

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

Yes, see the answer to question 3.3 regarding reports to the AML database about all bank transfers above a certain threshold.

3.13 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 discussed above, the Money Laundering laws apply in greater detail to entities working in the fields specified in the Third Addendum to the Law.

4 General

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

There is currently a private Bill in the Knesset in the initial stages of consideration, which seeks to impose a reporting obligation upon the providers of legal and business services (lawyers, trust companies, property companies and the like). This Bill was last discussed in the

Knesset in July 2017, and awaits further progress in the legislative timetable. The lack of such an extension of AML obligations to these sectors of the business economy was highlighted in the IMPA 2016 Annual Report, as being one of the gaps with full FATF compliance.

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?

Amendment 168 to the Israeli Tax Ordinance grants a 10-year exemption from filing tax returns and paying taxes on income earned abroad by new immigrants and returning residents. The purpose of this tax break is to attract Jews to immigrate to the State of Israel, and has been enshrined in law for many years. This provision includes a complete exemption on reporting foreign income. The 'Global Forum on Transparency and Exchange of Information for Tax Purposes' of which Israel is a member, produced a report in 2013 which stated that "Israel does not ensure availability of accounting records in respect of overseas activities of foreign companies that are managed and controlled in Israel by new immigrants or long-term returning ex-pats, for a period of ten years".

The Israel Tax Authority is seeking to amend two of what it perceives to be problematic clauses in amendment 168: the exemption it provides immigrants and returning Israelis on reporting income derived abroad; and a clause that says the finance minister can unilaterally publish regulations allowing the exemption to be extended for another ten years for individuals who meet certain criteria. The proposal is that in future, changes to these regulations would have to be approved by the Knesset Finance Committee.

The proposed changes have not yet been tabled in the Knesset.

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

Yes, the last report by Moneyval was published on 12 December 2013, based on their fourth visit to Israel. A further Moneyval visit to Israel took place recently in March 2018. A copy of the last report is available on the IMPA website.

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 laws and regulations are available in English on the Ministry of Justice website: http://www.justice.gov.il/En/Units/IMPA/Legistlation/Pages/default.aspx.

Dr. Zvi Gabbay
Barnea
58 Harakevet Street
Tel Aviv 6777016
Israel

Tel: +972 3 640 0600
Email: zgabbay@barlaw.co.il
URL: www.barlaw.co.il

Dr. Zvi Gabbay is a Partner and the Head of the Capital Markets Department at Barnea law firm. Prior to this, Dr. Gabbay served as the Head of Enforcement and a member of management at the Israel Securities Authority (ISA).

Zvi is an expert in the fields of financial regulation and securities enforcement, in both Israel and the United States. He now advises corporate clients on operations relating to capital markets, corporate and securities law, and international litigation.

Zvi also represents individuals and companies facing Israel Securities Authority administrative enforcement and criminal proceedings.

Zvi is dual USA/Israel qualified.

Adv. David Gilinsky
Barnea
58 Harakevet Street
Tel Aviv 6777016
Israel

Tel: +972 3 640 0600
Email: dgilinsky@barlaw.co.il
URL: www.barlaw.co.il

David Gilinsky is a lawyer in Barnea's Capital Markets Department, specialising in regulation, investments and funds. David advises regulated and private companies, based in Israel and abroad, on matters pertaining to the capital market, financial regulation, and commercial law.

David also advises on a range of EU regulation, including the new EU MIFID 2 and MIFiR requirements, EMIR and AIFMD. David is admitted to practise in Israel and England and Wales.

BARNEA

Barnea Jaffa Lande & Co. is a leading commercial law firm in Israel with an esteemed reputation in the international arena. About 70% of our firm's activities have an international dimension. The firm provides comprehensive legal services on financial regulation and enforcement in Israel and abroad. Clients include public companies traded on the Tel Aviv Stock Exchange and on foreign stock exchanges, dual-listed companies, companies seeking to delist, etc. Barnea also represents investment houses, provident and mutual funds, hedge funds, investment consultants, marketers and portfolio managers operating or looking to operate in Israel. Additionally, the firm represents numerous companies during initial coin offerings (ICOs).

Japan

Yamashita, Tsuge and Nimura Law Office

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?

Prosecutors belonging to the Public Prosecutor's Office are basically the only government agents in Japan that are allowed to prosecute anyone for a criminal offence, including 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?

The elements for the offence of money laundering are:

(1) (i) disguising facts pertaining to the sources, acquisition, or disposition of (ii) "Criminal Proceeds, etc.", which includes (a) Criminal Proceeds (defined in question 1.10), (b) property that is acquired in exchange of Criminal Proceeds, and (c) commingled property including Criminal Proceeds;

(2) the 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 the representative director or similar officer.

Accomplices or accessories to such crime are also punishable.

The predicate offences regarding 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 Organised Crime).

Yes, laundering the proceeds of foreign crime may be subject to punishment in Japan.

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

Both (i) the National Police Agency ("NPA"), and (ii) the government agency supervising the applicable industry area (e.g. the Financial Services Agency for the bank industry) are responsible for performing investigations and imposing administrative penalties. And if the NPA judges that a 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 for money laundering crimes is five years.

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

Yes, but 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 falls under any of the following may be confiscated:

(i) Instrumentalities of a 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.

(iv) Property of corresponding value of Criminal Proceeds in cases where the Criminal Proceeds are commingled with other property.

There is neither 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.

For example, in the Olympus fraudulent accounting case, the CEOs and other employees of two securities companies were arrested for money laundering offences, in which case they were reported to have transferred 2.2 billion yen worth of Criminal Proceeds to overseas investment funds, which they had received as remuneration for giving illegal advice on fraudulent accounting. This incident was very scandalous because the arrested persons included ex-employees of Nomura Securities, which is the leading securities company in Japan.

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 that enables plea bargaining will come into force on or before June 2, 2018.

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 law on money laundering, the "Act on Prevention of Transfer of Criminal Proceeds" ("AML Act"), was implemented by the congress. The cabinet enforcement order providing for the details of such law was set forth by the cabinet, and the cabinet enforcement ordinance providing for further details was set forth by the Commissioner General of the National Police Agency, the minister of the Financial Services Agency and other ministers for business areas that are subject to AML regulations.

Financial institutions and Designated Non-Financial Businesses and Professions ("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 Reports ("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?

The Japan Federation of Bar Associations implements a rule on AML measures to be followed 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 responsible for AML compliance and enforcement against their members.

2.4 Are there requirements only at the national level?

Yes, these 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? Are the criteria for examination publicly available?

This is the same as stated in question 1.4.

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 Financial Intelligence Centre of the NPA ("FIC") is the FIU in Japan. The FIC publishes an annual report of the results 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 limitations 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 individuals is imprisonment for up to two years and a fine of up to 3 million yen. The maximum penalty for legal entities is a fine of 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 licence, (ii) an order for suspension of business, and (iii) an order for rectification.

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

No.

Yes, they can be 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: there is no fine.

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, then one may file a lawsuit 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.

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, money 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, etc.

3.2 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 programme should basically 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) 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.

3.3 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 record-keeping requirement for transactions for financial institutions and DNFBPs. There are some exemptions to this requirement, including an exemption for transactions pertaining to 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.

3.4 Are there any requirements to report routine 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 on cross-border payments (as described further in question 3.5);
- Articles 55-3 and 55-4 provide for reports on 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.

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

For cross-border funds transfer in an amount exceeding 1 million yen, the relevant financial institution has to 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 amounts 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.

3.6 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 Transactions (for individual customers)

(a) having the customer present a photo ID document;

(b) having the customer present two types of non-photo ID;

(c) having the customer present a non-photo ID, and delivering transaction-related documents with non-transferrable certified mail to the address on such ID; or

(d) having the customer present a non-photo ID, and delivering transaction-related documents to the address on such ID.

* For legal entity customers, one needs to have the customer present an ID document (e.g. certification of the commercial registry) of such legal entity.

(ii) Main Methods of Verification of ID for Non-Face-to-Face Transactions (for individual customers)

(a) receiving a copy of the ID document, and sending a non-transferrable certified mail to the address on such document; or

(b) sending transaction-related document(s) to the customer's address, having an employee of the mail service business entity confirm the ID presented by the customer at the residence, and receiving information pertaining to statutory items from such employee.

** For legal entity customers, method (a) is possible. Also, one may receive certification from the commercial registry by electronic methods, pursuant to statutory procedures.

(iii) 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 opening of bank account, 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).

(iv) Other Items to be Verified

Other items which need to be verified include:

(a) the purpose of the transaction;

(b) identification of the agent and its authority as the agent;

(c) the occupation (in case of an individual)/the purpose (in case of legal entity); and

(d) identification of the substantial owner (in the case of a 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 the DPRK); or

(c) Transactions derived from Designated Transactions, 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 also need to be complied with:

(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 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 making transactions with Foreign PEPs.

3.7 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 shell banks is not permitted in Japan.

Also, banks and fund transfer businesses licensed or registered in Japan are required to make investigations into whether the financial institution with which it will enter into a correspondent agreement is a shell bank or not (Article 9 of the AML Act).

3.8 What is the criteria for reporting suspicious activity?

There are basically two types of transactions that are subject to submission of SARs. One type is transactions where the funds that the relevant financial institution or the DNFBP receives from the customer are suspected to be Criminal Proceeds, etc. The other type is transactions where the customer is suspected to be engaging in money laundering.

It should be noted that lawyers, accountants and similar professions are exempted from submitting SARs. They may submit SARs when they deem it necessary, but they are not obliged to do so under Japanese law.

3.9 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 and no. Japanese legal entities are registered in the commercial registry administered by the government. However, the names of shareholders are not registered in the commercial registry.

When a legal entity registers certain items requiring shareholder resolution, including appointment of corporate officers, the applicant will need to submit an attached document listing names of principal shareholders and other items to the registrar, and third parties may request to view such attached document if such third party has a special interest in such resolution. The Japanese government has given an interpretation, stating that the interest of financial institutions in conducting CDD appropriately may be considered in this respect, but the original purpose of such provision was not to facilitate CDD.

Thus, the commercial registry is imperfect for such purpose.

3.10 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 is basically interpreted not to apply to card transactions (e.g. Visa and MasterCard), as described in the Interpretive Notes to FATF Recommendation 16.

3.11 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 on a share certificate is not obligatory (Article 216 of the Companies Act), so bearer shares do exist and are not prohibited.

3.12 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.

3.13 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 differences, but they are not that significant.

(2) In relation to the Foreign Exchange and Foreign Trade Act, banks and funds transfer businesses are required to conduct CDD when providing cross-border wire transfers or other funds transfer services to their customers.

Also, banks, securities companies, currency exchange businesses, and certain other types of financial institutions are obliged to conduct CDD 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 to the CDD measures required under the AML Act.

Under tax-related laws, banks and securities companies are basically required to ask the "My Number" of the customer when opening an account, which is a social security and tax number given to each individual resident by the Japanese government. These companies are required to verify the My Number using a 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 has been publicised at the time of writing.

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) Finance lease and currency exchange businesses are not subject to any permit, licence, authorisation nor registration requirements.

(2) Transactions with "Domestic" Politically Exposed Persons are not deemed high-risk transactions.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Counsel 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 the following website: 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 during 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 Japan government website.

English translations of Japanese laws in general can be found on http://www.japaneselawtranslation.go.jp/?re=02. However, some laws or their most current versions have not yet been translated. It seems that it takes at least a year or two after a law's amendment before its translation is completed.

The following NPA website is also useful, but the content does not seem to be up to date: https://www.npa.go.jp/sosikihanzai/jafic/en/hourei_e/data/sekoukisoku2504.pdf.

For example, as of December 6, 2017, the translations of related acts on the above website are not up to date, and it does not reflect (i) the big amendment in 2015 regarding the methods of CDD, Foreign Politically Exposed Persons, internal control, correspondent agreements and such, nor does it reflect (ii) the amendment in 2016 obligating virtual currency exchange operators to conduct CDD and other such AML measures.

Ryu Nakazaki
Yamashita, Tsuge and Nimura Law Office
3F, Nishi-Shimbashi KS Building
1-16-3, Minato-Ku
Tokyo 105-0003
Japan

Tel: +81 3 3539 4651
Email: r-nakazaki@ytn.itplugin.net
URL: www.ytn-law.com/english

Partner, Yamashita, Tsuge and Nimura Law Office.

Specialising in the areas of (i) finance (money transfer, loan, card business, AML, Fintech, etc.), and (ii) internet businesses (advertisements, data businesses, internet malls, online games, PII, IP, etc.). Assisting clients in business collaboration agreements, licence agreements, and other transactions in the above areas and giving legal advice on regulations in Japan.

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.

Statutory Auditor of the Japan Online Game Association (2015–).

Has engaged in (i) the amendment of the credit card act (or the Instalment Sales Act), and (ii) supervision of related regulations, including AML, as a deputy director in the Japanese government.

Eight years in the U.S. (five years in New York and three years in California).

YAMASHITA, TSUGE & NIMURA

Yamashita, Tsuge and Nimura Law Office was founded in 1978 and advises many clients including major financial institutions and internet companies on various Japan-related laws, issues and transactions.

Kenya

Leah Njoroge-Kibe

Elizabeth Kageni

JMiles & Co.

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:

a) the accused person entered into or became concerned in an engagement or arrangement,

b) which he knew or ought to have known facilitated the acquisition, retention, use or control,

c) of criminal property (proceeds of crime),

d) 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 combating 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 the 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 combating 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 the 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? 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 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 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 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.

3.3 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)).

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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).

3.12 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.

3.13 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 combating 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, Counsel 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
Kenya

Tel: +254 20 434 3159 / +254 700 000 106
Email: lnk@jmilesarbitration.com
URL: www.jmilesarbitration.com

Leah Njoroge-Kibe is an 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
Kenya

Tel: +254 700 000 106 / +254 20 434 3159
Email: ek@jmilesarbitration.com
URL: www.jmilesarbitration.com

Elizabeth Kageni 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.

Significant clients of the firm include:

- Dowans Tanzania Limited
- Symbion Power Tanzania Limited
- Prime Fuels Limited
- WS Insight Limited
- Triumph Power Generating Company Limited
- Acacia Property Developers Limited
- Kenya Capital Markets Authority
- Lupain Group Inc
- GardaWorld (Kenya) Limited
- Adil Popat

Lebanon

Nada Abdelsater-Abusamra

Serena Ghanimeh

ASAS LAW

1 The Crime of Money Laundering and Criminal Enforcement

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

In 2001, the Anti-Money Laundering Law No. 318 was enacted, and in 2015 it was amended by Law No. 44 on Fighting Money Laundering and Terrorism Financing (hereinafter the "AML/CFT law").

In general, money laundering cases are referred to the General Prosecutor before the Court of Cassation, who will either classify the case if there are insufficient criminal components, or refer it to the General Prosecutor before the Court of Appeal for further investigation and prosecution as applicable.

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 predicate offences of Money Laundering are set out in the AML/CFT Law.

Article 1 of the AML/CFT Law defines "Illicit Funds". It includes assets, tangible and intangible, movable and immovable, including any legal documents or instruments evidencing title to, or interest in, such assets, resulting from committing, attempting to commit, or participating in the commission of any of the following offences whether in Lebanon or abroad:

1. The growing, manufacturing, or illicit trafficking of narcotic drugs and/or psychotropic substances according to the Lebanese laws.
2. The participation in illegal associations with the intention of committing crimes and misdemeanours.
3. Terrorism, according to the provisions of Lebanese laws.
4. The financing of terrorism or terrorist acts and any other related activities (travel, organisations, training, recruiting, etc.) or the financing of individuals or terrorist organisations, according to the provisions of Lebanese laws.
5. Illicit arms trafficking.
6. Kidnapping using weapons or by any other means.
7. Insider trading, breach of confidentiality, hindering of auctions, and illegal speculation.
8. Incitation to debauchery and offences against ethics and public decency by way of organised gangs.
9. Corruption including bribery, trading in influence, embezzlement, abuse of functions, abuse of power, and illicit enrichment.
10. Theft, breach of trust, and embezzlement.
11. Fraud, including fraudulent bankruptcy.
12. The counterfeiting of public and private documents and instruments, including cheques and credit cards of all types and the counterfeiting of money, stamps and stamped papers.
13. Smuggling, according to the provisions of the Customs law.
14. The counterfeiting of goods and fraudulent trading in counterfeit goods.
15. Air and maritime piracy.
16. Trafficking in human beings and smuggling of migrants.
17. Sexual exploitation, including of children.
18. Environmental crimes.
19. Extortion.
20. Murder.
21. Tax evasion, in accordance with the Lebanese laws.

Clearly, tax evasion is a predicate offence for money laundering.

According to Article 2 of the AML/CFT law, acts with the following purposes are considered as money laundering:

1. Concealing the real source of illicit funds, or giving, by any means, a false justification regarding the said source, with the knowledge of the illicit nature of these funds.
2. Transferring or transporting funds, or substituting or investing funds in purchasing movable or immovable assets or in carrying out financial transactions for the purpose of concealing or disguising the illicit source of such funds, or assisting a person involved in the commission of any of the offences mentioned in Article 1 to avoid prosecution, with the knowledge of the illicit nature of these funds.

Since the enactment of the AML/CFT Law, it has become clearer that money laundering is a separate offence that does not necessitate a charge with the underlying predicate offence.

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

Article 1 of the AML/CFT Law expressly states that the crimes listed therein constitute money laundering predicate offences, whether these crimes are committed within Lebanon or not.

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

Concerning the prosecution, see question 1.1 above.

Concerning the investigation of money laundering offences, these may be investigated by the prosecutor and the Instruction Judge. However, any financial/banking investigation aspects are carried out by the "Special Investigation Commission" (hereinafter "SIC") specialising in the investigation of money laundering. The SIC is an independent legal entity with a judicial status. It is established at the *Banque du Liban* (BDL — the Central Bank of Lebanon) and is empowered, *inter alia,* to receive and analyse suspicious transactions reports (STRs), to conduct financial investigations, to lift banking secrecy, to freeze accounts and/or transactions and forward information to concerned judicial authorities, in addition to other tasks. The SIC website can be visited at https://sic.gov.lb/en/.

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

Yes. Corporate criminal liability is governed by Article 210 of the Lebanese Penal Code.

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

According to Article 3 of the AML/CFT Law, the maximum penalties are seven years of imprisonment and a fine up to twice the amount laundered.

Under Article 210 of the Penal Code, legal entities may be convicted of confiscation, payment of fines and publication of the judgment.

Moreover, under Articles 108 and 109 of the Penal Code, legal entities other than public institutions may be suspended (and in certain cases dissolved) if their directors, administrators, representatives or agents commit, on behalf of these entities or by using a mean related thereto, an offence or a felony punishable by two years of imprisonment or more.

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

Money laundering lies in the category of "offences" (as opposed to felonies). As such, the statute of limitations for such crime is three years.

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

Lebanon is not a federation. Enforcement is 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?

As per Article 14 of the AML/CFT Law, the movable or immovable assets that a final Court ruling proves to be related to, or derived from, a money laundering or terrorism financing offence, shall be confiscated for the benefit of the State, unless the owners of the said assets prove in a Court of Law their legal rights thereupon.

As per Article 98 of the Lebanese Penal Code, the confiscation extends to things which fabrication, possession, sale or use are illicit even if they do not belong to the defendant or the convicted, and even if the prosecution did not entail indictment. Under the AML/CFT Law, with suspected money laundering transactions, the SIC may take precautionary and temporary measures such as the freezing of suspicious accounts and/or transactions, for a maximum period of one year, which is renewable for six months for foreign requests of assistance, and for a maximum period of six months, renewable for three months, concerning local requests of assistance.

Moreover, the SIC has the authority to permanently freeze accounts and/or transactions suspected to be related to money laundering. The SIC is also entitled to attach an encumbrance on the records and entries pertaining to movable or immovable assets, indicating that such assets are under investigation by the Commission.

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

We are not aware of a case where banks or other regulated financial institutions or 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?

In general, criminal actions are resolved or settled through 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.

Under the AML/CFT Law, the SIC is empowered to verify compliance by the banks, financial institutions, and various other businesses with the requirements provided for in the said law, and with the regulations issued in relation thereto (see question 3.1 below).

Moreover, as the regulator of the financial and banking sector, the BDL is empowered to issue regulations addressed to banks, financial institutions and other institutions regulated by the BDL, and oversee their implementations, namely the BDL Regulations attached to Basic Decision No. 83.

On the other hand, the Banking Control Commission of Lebanon ("BCC") (which is an administratively independent body, but in close coordination with the Governor of the BDL) has a main function to supervise banks, financial Institutions, exchange institutions and comptoirs. The BCC monitors notably the implementation of the BDL regulations and the International Accounting Standards.

According to Article 4 of the AML/CFT Law, banks, financial institutions and other institutions requiring a licence or supervised by the BDL, must comply with the following requirements and with

the regulations issued by the Banque du Liban in implementation of the said law:

1. To implement Customer Due Diligence measures on permanent customers (whether natural persons, legal persons, or those with a unique legal arrangement), in order to check their identity based on reliable documents, information or data.
2. To implement Customer Due Diligence measures on transient customers to verify their identity, if the amount of a single operation or series of operations exceeds the threshold designated by the Banque du Liban.
3. To determine the identity of the economic right owner and take the steps needed to verify his identity, based on reliable documents, information or data.
4. To keep copies of related documents of all operations, and to keep the information, data or copies of the customers' identification documents, for at least five years after performing the operations or ending the business relationship, whichever is longer.
5. To continuously monitor and review the business relationship.
6. To apply the measures outlined at items 1 to 5 above to permanent and transient customers, whenever there are doubts regarding the accuracy or adequacy of declared customer identification data, or whenever there is a suspicion of money laundering or terrorism financing, regardless of any thresholds or exemptions that limit the implementation of these measures.
7. To take into account the indicators that flag the likelihood of a money laundering or terrorism financing operation, as well as the due diligence principles to detect suspicious operations.

Moreover, in 2001 the BDL issued "Basic Circular No. 83" attaching the "Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing (AML/CFT)". The said Regulations set out the minimum rules to be followed by banks and financial institutions to avoid any involvement in operations related to money laundering or terrorist financing.

The Regulations were last amended in 2016 by the BDL intermediate circular No. 421.

In brief, the Regulations attached to Basic Circular No. 83: set out the measures to be implemented by banks when dealing with foreign correspondent banks abroad; regulated relations with customers; set out the due diligence measures and the policy related to beneficial owners; and outlined the risk indicators in this respect. It required the local banks to immediately notify the Governor of the BDL in his capacity as chairman of the SIC, when the bank holds evidence or has doubts that the attempted or preformed banking operation involves money laundering or terrorist financing or terrorist acts or terrorist organisations. The BDL website can be visited at http://www.bdl.gov.lb/.

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

According to Articles 5 and 7 of the AML/CFT Law, accountants, notaries, auditors and lawyers have the obligation to comply with the anti-money laundering requirements when performing specific activities on behalf of their clients. Concerning lawyers, the Beirut Bar Association issued a guideline manual which sets out the regulatory framework for certain operations carried out by lawyers, in light of the provisions of the AML/CFT Law. (See Section 3 below.)

The Association of Banks in Lebanon ("ABL") assists the banks in Lebanon in understanding and implementing the AML requirements.

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

Pursuant to Article 17 of the AML/CFT Law, the Ministry of Justice, and each of Beirut and Tripoli Bar Associations, the Lebanese Association of Certified Public Accountants ("LACPA") respectively are responsible for monitoring anti-money laundering compliance by notaries, lawyers and accountants. For example, and pursuant to the guideline issued by the Beirut and Tripoli Bar Association, the decision was made to establish the AML/CFT Compliance Committee within the Bar Associations whose prerogatives include the preparation of compliance reports and referral of said reports to the Bar Chair to take proper measures.

2.4 Are there requirements only at the national level?

Yes, there are requirements only at a national level.

However, the BDL Basic Circular No. 126 provides that Lebanese Banks must be fully informed of the laws and regulations governing their correspondents abroad, and deal with the latter in conformity with the laws, regulations, procedures, sanctions and restrictions adopted by international legal organisations or by the sovereign authorities in the correspondents' home countries. The violation of such requirements entails the application of the administrative sanctions stipulated in the applicable laws and regulations, particularly the sanctions stipulated in Article 208 of the Code of Money and Credit.

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

The Banque du Liban is the primary authority that issues regulations addressed to banks, financial institutions and all other institutions licensed or supervised by the BDL; and the latter are compelled to comply with such regulations.

Moreover, the SIC is the competent authority for examining compliance with anti-money laundering requirements (Article 6 of the AML/CFT Law).

Also, the BCC supervises banks, financial institutions, exchange institutions and comptoirs and monitors, notably with the implementation of BDL regulations and the International Accounting Standards.

Furthermore, Article 17 of the AML/CFT Law requires the auditors of banks, financial institutions and other companies and institutions mentioned in the said law, to verify the compliance by all these companies and institutions with the provisions of the said law and with the implementation regulations issued in relation thereto, and notify the chairman of the SIC of any violation thereto.

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?

The SIC is Lebanon's financial intelligence unit (FIU), established by the law No. 318 of 2001. The circulars issued by the SIC are published on the SIC's website at http://www.sic.gov.lb/en/internationalorginizations.

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

Please refer to our answer under 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?

According to Article 13 of the AML/CFT Law, the failure by the persons subject to anti-money laundering requirements to comply with the obligations/requirements set by the said law shall be punishable by imprisonment for a maximum period of one year, and by a fine of one hundred million Lebanese pounds maximum, or by either penalty.

The acts or omissions that are subject to these penalties include:

- Non-compliance with the requirements mentioned under question 2.1 above.
- The omission of reporting any suspicious activities to the chairman of the SIC.
- The omission of providing the SIC with all documents and information needed as per its request.
- Disclosing or insinuating to anyone that a suspicious transaction report or other relevant information is submitted or intended to be submitted to the SIC or that the SIC is inquiring about customers or auditing their operations or accounts.

Moreover, the Higher Banking Commission may impose on the parties that were referred to it a fine for non-compliance, with the regulations issued for the purpose of implementing the AML/CFT Law, provided that such fine does not exceed two hundred times the official minimum wage.

Additionally, the non-compliance with the BDL regulations will be subjected to special administrative sanctions pursuant to Article 208 of the Code of Money and Credit.

In fact, Article 208 of the Money and Credit Law No. 13513 (issued on 1/8/1963) states that if the bank breached the measures imposed by the BDL or has provided false or incomplete information, the BDL through the Higher Banking Commission may impose on the bank the following administrative sanctions:

1. Warning.
2. Reducing or suspending credit facilities.
3. Prohibiting the bank from conducting certain operations or imposing other limits.
4. Appointing a controller or an interim director.
5. Removing the bank from the list of banks.

And such in addition to any applicable fines or criminal sanctions imposed on the bank.

On the other hand, under Article 13 of the AML/CFT Law, the SIC may send a warning to entities who breach the regulations issued in implementation of the said law, and request from them reports on the measures taken to redress their situation. The SIC may also refer these entities to the Higher Banking Commission.

In this context, the SIC Circular No. 15 of 2014 addressed to banks and financial institutions states that any bank or financial institution that violates the AML provisions shall incur the administrative penalties that the Higher Banking Commission may impose, in accordance with Article 208 of the Code of Money and Credit. These penalties shall not preclude the enforcement of penal sanctions and civil liability against the violating entity.

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

See question 2.8 above.

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

See 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?

The SIC conducts the necessary audit and analysis, further to which the SIC shall decide to permanently freeze the concerned accounts and/or transactions, and/or to lift the banking secrecy in favour of the competent judicial authorities and the Higher Banking Commission, and to keep suspicious accounts as traceable accounts. The SIC may withdraw any of its decisions, in whole or in part, if it obtains any new relevant information (Article 6.3 of AML/CFT Law).

As for the decisions of the Higher Banking Commission (see question 2.8 above), these cannot be appealed or objected before any administrative or judicial authority. Note that under Article 210 of the Money and Credit Law, the decisions of the Higher Banking Commission regarding the appointment of a temporary director or the removal of the bank from the list of banks shall be published.

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.

Under Article 4 of the AML/CFT Law, the following institutions are subject to anti-money laundering requirements: banks, financial institutions, leasing companies, institutions that issue and promote credit or charge cards, institutions that perform money transfers electronically, exchange institutions, financial intermediation institutions, collective investments schemes, and any other institution requiring a licence or which is supervised by the Banque du Liban.

Moreover, Article 5 of the same Law requires institutions that are not subject to the Banking Secrecy Law of 3 September 1956, particularly insurance companies, casinos, real estate dealers and agents, and merchants of valuable materials (jewellery, precious stones, gold, works of art, antiques) to keep records of operations that exceed the threshold specified by the SIC. The said institutions must also comply with the obligations specified in Article 4 of the said law (see question 2.1) and with the regulations and recommendations issued by the SIC for the purpose of implementing the provisions of the said law.

Additionally, the SIC Circular No. 1 addressed to states that all institutions not governed by the Banking Secrecy Law of 3/9/1956,

including individual institutions, and particularly money dealers, financial brokerage firms, leasing companies, mutual funds, insurance companies, real estate development, promotion and sale companies, and high-value items merchants (jewellery, precious stones, gold, works of art, archaeological artefacts) must abide by the provisions of the AML Law.

Article 5 also provides that certified accountants and notaries must comply with the anti-money laundering requirements when performing specific activities on behalf of their clients, such as the buying and selling real estate and the managing of bank and securities accounts.

Furthermore, Article 5 states that the said requirements will apply to lawyers when carrying out the activities mentioned here above according to the mechanism to be set by the Beirut Bar Association and the Tripoli Bar Association, taking into account the particularities and rules of the legal profession. On 20 April 2017, the said associations jointly issued a manual setting out the regulatory framework for certain operations carried out by lawyers in light of the provisions of the AML/CFT Law. The manual became effective on 1 October 2017.

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

As per Article 10 of the Regulations attached to Basic Circular No. 83, each bank operating in Lebanon must establish an AML/CFT Compliance Unit.

Article 11 of the said Basic Circular states that the said Unit must comply with various procedures aiming at controlling, fighting and preventing money laundering, including:

- Preparing a procedure guide on the implementation of the AML/CFT Law and the Regulations.
- Preparing a form for customer's identification (KYC: Know Your Customer).
- Verifying the proper implementation and effectiveness of AML/CFT procedures and regulations.
- Preparing a staff training program concerning the methods of controlling financial and banking operations, in order to fight money laundering and terrorist financing.
- Ascertaining that concerned employees are complying with the procedure guide on the implementation of the AML/CFT Law legal and regulatory texts, and that the KYC forms are filled out, and to prepare reports to this effect.

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

As per Article 4 of the AML/CFT Law and BDL Regulation No. 83, banks and financial institutions must keep copies of related documents of all operations, and keep the information or data or copies of the customers' identification documents, for at least five years after performing the operations or ending the business relationship, whichever is longer.

Moreover, the institutions not governed by the Banking Secrecy Law outlined under SIC Circular No. 1 (see questions 3.1) must keep special records for operations, the value of which exceeds ten thousand US dollars or equivalent.

As for filing reports, Article 7 of the AML/CFT Law states that the persons subject to the said law on anti-money laundering requirements, including certified accountants and notaries, must promptly report to the chairman of the SIC the details of the operations undertaken or attempted to be undertaken that are suspected to be related to money laundering or terrorism financing. Moreover, the supervisors of the Banking Control Commission must, through the chairman of the latter, report to the chairman of the SIC any operations they suspect to be related to money laundering or terrorism financing and which they are aware of while performing their duties.

Moreover, the SIC Circular No. 1 mentioned here above provides that the institutions not governed by the Banking Secrecy Law must report any suspicious money laundering operations in accordance with the form attached thereto.

It follows that the reporting requirement imposed by the AML regulations apply to any suspicious money laundering operation, irrespective of its amount.

3.4 Are there any requirements to report routine 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 mentioned under question 3.3 above, reports must be filed on any suspicious money laundering operation; there are no dollar thresholds for reporting suspicious operations.

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

BDL Basic Circular No. 69 issued in 2000 addressed to banks, financial institutions and institutions performing electronic banking and financial operations states that these banks and institutions must communicate to the SIC the details of any doubtful operation that may involve money laundering or terrorism financing.

Moreover, all persons transporting physically, in or out of the border, currency/negotiable instruments on them in their accompanying luggage, or by any other means, must submit a written declaration thereon to the Customs authorities whenever the value exceeds the amount of USD 15,000 or its equivalent in other currencies (Article 2 of Law No. 42 of November 24, 2015 on "Declaring the Cross-Border Transportation of Money").

3.6 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?

Banks must adopt clear procedures for opening new accounts and must apply due diligence measures including: checking the identity of their permanent and transient customers, whether resident or non-resident; determining the purpose and the nature of the relation or of the account opening; identifying the beneficial owner and the source of funds; and ensuring the ongoing control of operations (Article 3 of the Regulations attached to Basic Circular No. 83).

Moreover, regardless of the amount involved, the employee in charge of performing the operation must check the identity of the customer when noticing that, on the same account or on multiple accounts held by the same person, several operations are being carried out for amounts that are separately less than USD 10,000 but totalling or exceeding USD

10,000 or its equivalent in any other currency. Generally, the process requires collection of prescribed information and verification of that information from reliable and independent documents.

The said information must be retained by the bank at least for five years after closing the account or ending the business relation.

Additionally, when the bank suspects that the customer is not the beneficial owner or when the customer states that the beneficial owner is a third party, the bank must collect information related to the beneficial owner (Article 4 of the AML/CFT Law).

Banks and financial institutions are required to increase KYC level, including obtaining more detailed information about the customers and the operations, when these are classified as high risk according to risk scoring.

Moreover, banks and financial institutions must apply enhanced due diligence (increased KYC levels), in various cases, for example (i) when the bank suspects that the customer is not the beneficial owner, (ii) with respect to certain business sectors or persons considered as high risk, for example, foreign politically exposed persons, offshore companies and companies established in countries known to be tax havens, (iii) when accepting a check drawn on it by an exchange institution, or when performing operations requested by an exchange institution, and (iv) when requested to execute a transfer resulting from an exchange operation, or from a cross-border transportation of cash and/or precious metals to a third person in Lebanon, regardless of the amount being transferred (BDL Regulation No. 83).

3.7 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?

Article 2 of the Regulations attached to Basic Circular No. 83 provides that when establishing a relation with a foreign correspondent bank, the bank must ascertain that the correspondent bank is not a shell bank, that it really exists based on documentary evidence, and that it does not deal with shell banks. The bank must also ensure that the correspondent bank has a good reputation and is subject to a good control, implementing sufficient and effective procedures to fight money laundering and terrorist financing.

3.8 What is the criteria for reporting suspicious activity?

Article 5 of the Regulations attached to Basic Circular No. 83 requires banks to immediately notify the Governor of the Banque du Liban in his capacity as chairman of the SIC, when they hold evidence or have doubts that attempted or performed banking operations involve money laundering or terrorist financing or terrorist acts organisations, **especially**:

- When banks have persistent doubts about the veracity of the written statement submitted by the customer regarding the beneficial owner's identity, or that false or inaccurate information was given about this identity.
- When banks realise that they were misled in the course of checking the identity of the customer or of the beneficial owner, and have persistent doubts about the information provided by the customer.
- When transferred amounts or checks are returned, whether directly or upon the request of concerned parties, particularly correspondent banks, either because of forgery or because of doubts that they involve suspicious operations.

Moreover, Article 8 (a) of the same Regulations provides for sixteen indicators giving rise to suspicious matters, **for example**:

- Making large deposits or recurrent deposits which are unjustified by the customer's apparent business activity.
- Operating the account mainly to transfer large amounts abroad, or to receive a large transfer, when such operations are unjustified by the customer's activities.
- The replacement of large cash amounts by electronic transfer by banker's cheques.
- A change in the pattern of deposit operations made by a customer exempted from filling the cash transaction slip (CTS).
- The undertaking by a customer of large cash operations in the form of deposits and withdrawals, with insufficient personal identification.
- The holding by the customer of several accounts unjustified by the nature of his activities, or the undertaking of numerous cash transfers between and through these accounts.
- The occurrence of cash deposits and/or bank transfers, while the customer's activities do not generate a volume of funds.
- E-banking operations that appear unusual.

3.9 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 Lebanese companies and companies working in Lebanon must be registered at the Commercial Registry. This registry is under the supervision of the competent commercial court, available to the public and contains information about Lebanese and foreign legal entities working in Lebanon, such as their management and ownership. Any amendment or update related to these legal entities should be notified to the commercial registry. Failure to comply with such obligation entails the application of fines (Articles 27 and 37 of the Lebanese Code of Commerce).

Pursuant to BDL regulations, banks and financial institutions have to maintain records of the beneficial owners of legal entities/ arrangements.

3.10 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, accurate information about originators and beneficiaries should be included in payment orders and payment instructions.

Additionally, the BDL Basic Circular No. 69, issued in 2000, addressed to banks, financial institutions and institutions performing electronic banking and financial operations, expressly requires institutions performing electronic funds transfers to accurately insert in the transfer order and attached messages, the full identity of the ordering party (name and address), the account number or reference number in the absence of an account number, the sources of the funds, their destination and purpose, in addition to the identity of the beneficiary and the economic right owner, as the case may be.

These institutions should provide the competent authorities with all the above information within three working days from their request date.

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

Further to the enactment of Law No. 75 dated 27/10/2016, the ownership of legal entities in the form of bearer shares are prohibited.

Moreover, the BDL Intermediate Circular No. 411 dated 29/2/2016, prohibits banks, financial institutions, exchange institutions and leasing companies from performing any kind of banking or non-banking, financial or non-financial, exchange or non-exchange operations, as applicable, whether recorded in or off-balance sheet, with companies or mutual funds whose stocks and shares are totally or partially issued in bearer form, or with companies or mutual funds that are directly or indirectly owned by companies or mutual funds whose stocks and shares are totally or partially issued in bearer form.

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

See question 3.1.

3.13 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?

Certain business sectors or persons are considered as high risks entailing further measures of due diligence. The following are examples provided by Article 9 of Basic Circular No. 83:

- Foreign politically exposed persons who hold or have held important official positions (PEPs), their family members and close associates.
- Offshore companies.
- Companies established in countries known to be tax havens.
- Customers who are nationals or resident in countries that do not or insufficiently apply the FATF Recommendations.

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 legal framework in Lebanon was undertaken between 2001 and 2016, which resulted to an overhaul of the AML Law to comply with the latest international standards and best practices.

Indeed in 2016, the Law on tax requirements for trustees and the Law abolishing bearer shares and shares to order (Laws No. 74 and 75) were enacted. In addition to the Law on the exchange of information for tax purposes (Law No. 55). Moreover, the BDL Basic Circular No. 83 was amended so as to establish at banks an AML/CFT Committee at the board level, and various other circulars in this respect.

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 was conducted by the World Bank and was then discussed and adopted by the Plenary of the MENAFATF as a 1st mutual evaluation on 10 November 2009. The Ratings of Compliance with FATF Recommendations are exhibited under Table 1 of said Report available on MENAFATF's website: http://menafatf.org/information-center/menafatf-publications/mutual-evaluation-report-lebanese-republic.

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

Yes. Lebanon is a member of the MENAFATF. A Mutual Evaluation Report was conducted by the World Bank and was then discussed and adopted by the Plenary of the MENAFATF as a 1st mutual evaluation on 10 November 2009, which was followed by various follow-up reports, the latest being issued in April 2017. This report can be viewed at http://menafatf.org/information-center/menafatf-publications/mutual-evaluation-report-lebanese-republic.

Lebanon was also evaluated by the IMF and the OECD.

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 concerning anti-money laundering are published on the website of Banque du Liban at: http://www.bdl.gov.lb/, and on the website of the SIC: https://sic.gov.lb/en/. Most of the materials are available in English.

Nada Abdelsater-Abusamra
ASAS LAW
KALOT Building, 170, Museum Street
Facing Military Hospital, Badaro
Beirut
Lebanon

Tel: *+961 1 384556-7-8 / +961 3 363663*
Email: *nada.abdelsater@asaslaw.com*
URL: *www.asaslaw.com*

Nada Abdelsater-Abusamra is the Founder and Managing Partner of Abdelsater-Abusamra & Associates – ASAS LAW. She is an international lawyer admitted to the Courts of New York, Beirut and to the Special Tribunal for Lebanon; The Hague (Netherlands).

She is consistently ranked as a top lawyer by the most renowned international guides such as *Chambers Guide* and *The International Financial Law Review* (IFLR).

She handles major corporate and financial transaction including M&A, Corporate, Banking & Finance, Oil and Gas, Infrastructure, PPP, BOT, Tax, real estate and Telecoms. She also specialises in white collar crimes and anti-money laundering and asset recovery cases and she was recognised by *Who's Who Legal* in asset recovery.

Nada is the exclusive representative of "ICC-FraudNet", the London based Commercial Crime Services unit of the International Chamber of Commerce (ICC).

She is the first Arab woman to be elected to the international board of Transparency International (sitting in Berlin). She is the recipient of the Corporate Governance Rising Star Award, 2009, Yale University (School of Management, the Millstein Center).

She holds a Master of Laws from Harvard Law School, LL.M. and a French and Lebanese Master of Laws from Université St Joseph, Bachelor of Science from the American University of Beirut and completed coursework Masters in International Affairs at the Lebanese American University.

Serena Ghanimeh
ASAS LAW
KALOT Building, 170, Museum Street
Facing Military Hospital, Badaro
Beirut
Lebanon

Tel: *+961 1 384556-7-8*
Email: *serena.ghanimeh@asaslaw.com*
URL: *www.asaslaw.com*

Serena Ghanimeh has been a partner in Abdelsater Abusamra & Associates – ASAS LAW since 2013. She is a corporate attorney with eighteen years of experience. Her practice focuses on contracts law and arbitration.

She also advises on corporate structuring, employment and maritime law.

Fluent in English, French, Arabic and Spanish, she studied at St. Joseph University (Master of French and Lebanese Laws). She has been a member of the Beirut Bar Association since 1999.

ASASLAW
ABDELSATER ABUSAMRA & ASSOCIATES

ASAS LAW was founded in 2005. It is a specialist law firm gathering a team of sharp and highly experienced lawyers admitted to practise in New York, The Hague and Beirut.

The firm provides a full range of legal services to major leading international and national companies locally and across borders. It is the exclusive representative of ICC FraudNet advising on asset recovery and money tracing.

The firm is particularly renowned for handling complex M&A deals and transactions in various sectors including the energy sector, infrastructure and industry sectors.

The lawyers at ASAS LAW are professional deal makers providing breakthrough solutions using their creativity, experience and legal skills.

The firm has a unique reputation in international arbitration and mediation, as well as international and national litigation.

The firm is recognised as a market leader by reputable global legal directories, including *IFLR* and *Chambers & Partners* for its expertise, success and achievements in Corporate and Finance as well as in Arbitration and Dispute Resolution.

Luxembourg

DSM Avocats à la Cour

Marie-Paule Gillen

1 The Crime of Money Laundering and Criminal Enforcement

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

The State Prosecutor is the competent authority to prosecute money laundering. Pursuant to art. 23 (3) of the Penal Procedure Code, the FIU or the Control Authorities (as described below, see question 2.1) must inform the Prosecutor as soon as they are aware of or have a suspicion of any money laundering or terrorist financing act.

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 Prosecutor must prove the presence of both the material elements and the intentional element of the offence.

As to the material elements, he must prove that the accused has facilitated the false justification of the nature, the origin, and location of assets originated by predicate offences of money laundering, or that he has participated in a transaction aiming at investing, dissimulating the transfer or conversion of such assets, or has acquired, held or used these assets.

He must have committed such acts knowingly, i.e. he must have known (or presumed to have known) that he was involved in a criminal activity (intentional element).

A long list of 27 predicate offences is set forth in article 506-1 par. 1) of the Penal Code, covering a wide variety of serious crimes, with a final residual category being all crimes punished by a imprisonment of a minimum in excess of six months.

Two serious tax crimes, defined as tax embezzlement (*escroquerie fiscale*) and aggravated tax fraud (*fraude fiscale aggravée*) are also predicate offences of 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, money laundering is punishable in Luxembourg as soon as any material element of the offence has taken place in the Grand Duchy of Luxembourg, even if the predicate offence was committed abroad.

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

The State Prosecutor Office is the government authority responsible for prosecuting these offences. In accordance with the penal procedure code, he may seize an investigating judge with the task to conduct an enquiry on the facts and alleged offences.

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

Corporate criminal liability has been provided by law since 2010.

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

Money laundering is punished by imprisonment of a minimum of one year, up to five years maximum, and/or by a fine of 1,250 euros up to 1,250,000 euros. The period of imprisonment is aggravated to a period of 15 to 20 years if the offences are in participation with an association or an organisation.

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

Ordinary statute of limitations rules of the Penal code are applicable, i.e. 10 years for crimes and five years for delictual offences. The starting point of the period of limitations is the moment when the offence was committed.

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

No, the State Prosecutor Office is the only authority vested with the power to enforce the law from a penal law point of view. However, depending on the location of the facts qualified as offences, there are two possible competent prosecutor offices: the Prosecutor Office at the District court of Luxembourg, and the Prosecutor Office at the District court of Diekirch. There is no other district court in the 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?

Article 32-1 of the Penal Code provides for the special forfeiture (*confiscation spéciale*) of assets in case of money laundering. The assets subject to forfeiture are all the proceeds or assets, tangible or intangible, being the object of the offence or directly or indirectly deriving from the offence, or which are a patrimonial advantage deriving from the offence, as well as any goods which were substituted to these goods, plus their income, or any assets belonging to the convicted person. The forfeiture is pronounced by the court.

The forfeiture may be pronounced even in case of acquittal of the prosecuted person or in case of a time bar of the public action.

Forfeited assets may be rendered to a person who is victim to the offence or a damaged third party, pursuant to a decision of the court.

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, we are not aware of any conviction of money laundering of a bank or a banker or any other regulated financial institution.

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 the Penal Procedure Code, if mitigating circumstances are recognised and only in cases where the imprisonment does not exceed five years, a procedure called "judgement on agreement" (*jugement sur accord*) may take place. This procedure is conducted with the agreement of the State prosecutor and the decision is taken by the criminal court (*Chambre correctionnelle*).

We are not aware of any settlements or any other way of non-judicial conflict resolutions which would have been applied in the case of bankers prosecuted for money laundering.

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 law recognises three Control Authorities:

- The Commission de Surveillance du Secteur Financier (CSSF) for credit institutions or financial institutions or other professionals of the financial sector.
- The Commissariat aux Assurances (CAA) for professionals of the insurance sector.
- The Administration de l'Enregistrement et des Domaines (AED) for all other professionals not supervised or monitored by one of the above authorities or by a self-regulatory body.

The legal requirements consist mainly in the obligations (i) to proceed to customer due diligence by applying a risk based approach, (ii) to establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping and internal control, risk assessment, risk management, compliance management and communication, (iii) to ensure awareness and training of the employees, and (iv) to put in place systems in order to respond rapidly to the authorities' enquiries.

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

Yes, there are self-regulatory bodies' (SRB) rules applying to the members of legal professions, notaries, bailiffs, external auditors/ audit firms and external accountants.

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

Yes, the respective SRB are: the Luxembourg Law Society (*Ordre des Avocats*) for the attorneys at law, the Chamber of Notaries for notaries, the Institute of Auditors for statutory auditors or audit firms, the Chamber of Bailiffs for bailiffs, the chamber of accountants (*Ordre des Experts comptables*) for independent/external accountants

2.4 Are there requirements only at the national level?

Yes, the requirements are applicable at national level only.

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

The authorities and SRBs cited above are responsible for monitoring the compliance of their AML/FT obligations by the professionals in their scope of competence.

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 Financial Intelligence Unit of the State Prosecutor Office of the District Court of Luxembourg (FIU) is responsible for analysing the information reported by all professionals subject to the AML/ FT Law 2004.

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

No statute of limitations is provided in the AML/FT law of 12 November 2004 as amended (the AML/FT law 2004).

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?

Failures to comply with all AML/FT obligations as described above may be punished by administrative fines.

The maximum amount of the fine is twice the benefit obtained by the breach of the obligation or if this benefit is not ascertainable, one million euros.

If the professional involved is a credit institution or a financial institution, the maximum amounts of the fines are increased as follows:

- for legal persons: five million euros or 10% of the annual total turnover of the last financial year; and
- for natural persons: five million euros.

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

Various other types of sanctions or administrative measures are available to the authorities:

- a warning;
- a blame;
- a public declaration mentioning the identity of the persons concerned and the nature of the breach;
- a withdrawal or temporary suspension of the authorisation to exercise the activity (when an activity subject to an authorisation is concerned); and
- if the activity is subject to the authorisation of the CSSF (financial sector activity) or the CAA (insurance sector activity) those authorities have to power to temporarily prohibit the exercise the activity or management functions as the case may be, for a period which cannot exceed five years.

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

Violation of AML/FT obligations are also subject to criminal sanctions (consisting exclusively in financial fines) if they were committed intentionally. The amount of the fine ranges between 12,500 euros to five million euros.

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 fines and other administrative sanctions, when they are final, are published by the control authorities on their websites. However, the authorities may refrain from publishing their decision if the publication could harm the stability of the market or if it would be disproportionate.

The fines and other administrative sanctions are enforced by the AED. The AED has the power to recover the moneys due from fines applied by the control authorities.

A right of appeal against the sanction decision is available before the administrative court. It must be filed within one month from the date of notification of the decision.

All resolutions of penalty actions handled by the authorities are public.

We are not aware of a financial institution that has challenged penalty assessments in judicial or administrative 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 credit institutions, investment firms and all other professionals of the financial sector licensed or authorised to exercise their activities in Luxembourg, as well as payment institutions and electronic money institutions, insurance undertakings and insurance intermediaries acting in respect of life insurance, undertakings for collective investment (UCITS and UCIS), investment companies in risk capital (Sicars) and management companies of UCITS or UCIS. All these professionals except for the credit institutions are referred to as "financial institutions". Moreover, pension funds, managers and advisors of UCITS, UCIS, Sicars and pension funds, securitisation undertakings and insurance and reinsurance undertakings, alternative investment funds managers (AIFM), real estate agents, freeport and any other financial institutions not cited above and which conduct one of the activities described in the annex 1 to the AML/FT 2004 (which lists all of the financial or ancillary activities as defined by EU Banking Directive).

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

All financial institutions and other professionals in the scope of the AML/FT law 2004 are required to establish and maintain compliance programmes, which are part of their internal AML policies and procedures. The compliance programmes will include client acceptance rules and mechanisms, internal analysis and advice on compliance, program of controls and remediation of failures, procedure of cooperation with legal authorities, including suspicious transactions declarations, and training programmes for the employees.

The professional are required to set up these programmes which must be adequate and appropriate, and in proportion to their own risk, their nature and their size.

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

There is no fixed threshold applicable to all large transactions. Professionals must determine their own risk appetite, and determine what is a "large" transaction, taking into account his own business environment. This factor must be one of the elements of his appreciation of his risk. An unexpected or unexplained large transaction will certainly be a factor of risk and trigger an enhanced due diligence obligation from the professional.

3.4 Are there any requirements to report routine 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.

Any routine reporting to be made internally is determined by each

professional (obliged entity) according to its own risk appetite and its internal procedures.

There is no routine obligation of transaction reporting to the FIU.

According to the FIU Guidelines issued in January 2017, a suspicious transaction report (STR) must take place each time that the professional knows or has good reasons to suspect that a money laundering or terrorist financing transaction is taking place or has taken place, on the basis of factual elements such as the person involved, his or her evolution, the origin of the assets, the nature, the finality or modalities of the transaction. It is sufficient for the professional to have a negative impression, on the basis of circumstances, and he does not need to have any evidence available.

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

There are no cross-border transaction reporting requirements. STR must be lodged uniquely at the Luxembourg FIU.

3.6 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 process entails full identification of the client and of the ultimate beneficial owner, and verifications of the same to an extent that is proportional to the risk. In case of some factors of potential higher risk are detected, the professional must apply enhanced due diligence. Factor of potential higher risk are listed (as a non-exhaustive list) in Annex IV to the AML/FT law: they cannot be linked to the person of the client (e.g. a PEP or a resident in a non-FATF compliant country), or linked to the type of product or service (e.g. private banking, products which favour anonymity) or geographical factors (e.g. countries where corruption risks are very high, or countries under embargo).

3.7 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?

Any business relationship with shell banks is totally prohibited.

3.8 What is the criteria for reporting suspicious activity?

See question 3.4 above.

3.9 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?

Two Registers of Beneficial Owners will be created shortly according to bills of law which are about to be adopted. The first one (held at the Register of Commerce and Companies) concerns ultimate beneficial owners of companies or other legal persons, and the second one (held at the AED) concerns ultimate beneficial owners of trusts and fiduciary contracts.

3.10 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, these requirements of accurate information on the payer and the payee of funds transfers are applicable pursuant to the EU Regulation 2015/847, which is directly applicable in Luxembourg.

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

Bearer shares are permitted but companies which have issued bearer shares are subject to the obligation to appoint a depository of their bearer shares, which holds a register of such shares. The holders must deposit their shares with such depository.

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

Apart from the due diligence and cooperation with the authorities obligations applying to all obliged entities, including legal professions, notaries, bailiffs etc., there are some minimum thresholds triggering the obligation to identify the clients: for any professional carrying out occasional transactions of 15,000 euros or more, for traders of goods (10,000 euros) and for casinos and other hazard games if a gain of 2,000 euros or more is realised.

However, no reporting other than STR, and namely no currency reporting, is required.

3.13 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?

When professionals are engaged in business sectors or with persons or entities established in third countries which are not FATF-compliant, or do not present a comparable level of protection against money laundering and terrorist financing, they are obliged to apply an enhanced customer due diligence process.

Persons engaged in a free trade zone are subject to the AML/FT law 2004. (This concerns only one freeport operating company for the time being.)

4 General

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

The proposal of Fifth AML/FT EU directive is expected to be adopted shortly. This new directive will bring some major amendments to the existing AML/FT law 2004.

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 issued on 14 February 2014 its 6th follow-up report on Luxembourg. The FATF recognised that Luxembourg has made significant progress in addressing deficiencies identified in the February 2010 mutual evaluation report and decided that the country should be removed from the regular follow-up process.

According to the FATF recommendations and the 4th AML/FT Directive, stress will be put by the CSSF on the effectiveness of the AML internal controls and the external auditor's annual reports will have to cover the efficiency of the controls. The same issue will be borne in mind in the CSSF on-site visits.

Moreover, the CSSF has recently announced that it will conduct a new annual online survey collecting standardised key information concerning AML/FT risks, in order to include them in the risk-based approach of the CSSF.

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

The FATF issued on 14 February 2014 its 6th follow-up report on Luxembourg. The FATF recognised that Luxembourg has made significant progress in addressing deficiencies identified in the February 2010 mutual evaluation report and decided that the country should be removed from the regular follow-up process.

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 information on AML/FT legislation and regulations applicable to the professionals of the financial sector is published in English on the CSSF website: http://www.cssf.lu/en/supervision/financial-crime/.

Information concerning laws and regulations applicable to all sectors is also available on the FIU website but only in the French language: http://www.justice.public.lu/fr/organisation-justice/ministere-public/parquets-arrondissement/lutte-anti-blanchiment/index.html.

Marie-Paule Gillen
DSM Avocats à la Cour
55-57, rue de Merl
L-2146
Luxembourg

Tel: +352 26 25 62-1
Email: mpgillen@dsm.legal
URL: https://www.dsm.legal/en/

Partner / Attorney-at-law

Practice areas:

- Banking and Financial Law.
- Capital Markets.
- Compliance and Regulatory in the Financial Sector.
- Criminal Law and White Collar Crime.

Career:

2012: Attorney-at-law with the Luxembourg Bar and the Bar of Brussels; Partner, DSM *Avocats à la Cour*.

1997-2012: Secretary General and Chief Legal Officer of KBL European Private Bankers S.A. et Groupe.

1980-1997: In-house legal counsel/Head of Legal Department of KBL Luxembourg (renamed KBL European Private Bankers S.A.).

1980: Attorney-at-law, Luxembourg Bar.

1975-1980: Attorney-at-law, Bars of Brussels and Arlon (Belgium).

Education:

1995: International Banking School (summer session), Oxford (UK).

1989: International Banking Summer School, Trinity College, Dublin (Ireland).

1980: Graduate in Luxembourg law.

1975: University of Geneva: specialisation in European companies law and international law (Switzerland).

1974: University of Namur and Louvain: Master's in law/specialisation in economic law (Belgium).

Languages:

French, English, German, and Dutch.

DSM AVOCATS A LA COUR

DSM Avocats à la Cour is a middle-sized law firm in Luxembourg. Located in the heart of one of the world's main financial centres, DSM provides its national and international clientele multidisciplinary, multilingual services suited to Luxembourg's current environment. DSM's lawyers are recognised experts in numerous legal practice areas such as corporate finance, real estate and maritime law, as well as in dispute resolution.

The lawyers in each practice area have extensive training and thorough knowledge of their practice areas. They rely on their experience, constantly updated professional information and the firm's pragmatic and pluridisciplinary approach.

DSM Avocats à la Cour is a member of several independent international legal networks of partner law firms located throughout the world.

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?

Yes, 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*).

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 2/2006 (Prevention and suppression of the crime of money laundering) and Article 6 of Law 3/2006 (Prevention and suppression of the crimes of terrorism), as amended by Law 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 the 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 objective of Law 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 or 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.

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 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.
  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) 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.
  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?

Yes. 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 2/2006).
- The Housing Bureau (real estate intermediaries and agents).
- Macau Economic Service (other entities).

2.4 Are there requirements only at the national level?

Yes, they are. The requirements are only at the Macau Special Administrative Region's level.

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

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 2/2006. It is an independent government entity directly under the supervision of the Secretary for Economy and Finance.

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

The applicable statute of limitations is 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 5,000,000, 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?

Yes. 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 public. As to the criminal resolutions, they are public only 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 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

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

Bearer shares were eliminated by Law 4/2015 and are no longer permitted.

3.12 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.

3.13 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?

This is not applicable in Macau.

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, Counsel 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
Macau Landmark Office Tower, 23rd Floor
Avenida da Amizade 555
Macau SAR

Tel: +853 2856 2322
Email: cortes@lektou.com
URL: www.lektou.com

Pedro Cortés has been a lawyer at Rato, Ling, Lei & Cortés since 2003 and a partner since 2006, having extensive experience in gaming, corporate, finance and IP law.

Pedro has professional membership 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.

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 / Lektou Portugal
Avenida da República, n.6, 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 Lawyer at Rato, Ling, Lei & Cortés and has professional membership 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 Scientific 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.

律師事務所 RATO LING LEI & CORTÉS ADVOGADOS E NOTÁRIOS 私人公證署

Rato, Ling, Lei & Cortés – Lawyers (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 itself 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 demands of the firm's worldwide clients.

Philippines

Roberto N. Dio

Castillo Laman Tan Pantaleon & San Jose Law Offices

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 or 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, Section 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, Section 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, Section 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, Section 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. Thus, the crime of money laundering must be committed within the Philippine territory for it to be punishable under the AMLA.

However, the money laundering of proceeds of foreign crimes is punishable under the AMLA (*AMLA, Section 3(i)(34)*). Nevertheless, any element of the money laundering offence must still be committed within the territory of the Philippines for it to be punishable under the AMLA.

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

The AMLC is the government authority primarily tasked with implementing the AMLA. As part of its functions, the AMLC may investigate suspicious transactions (*AMLA, Section 7(5)*) and institute civil forfeiture proceedings and all other remedial proceedings through the Office of the Solicitor General ("OSG") (*AMLA, Section 7(3)*). It may impose administrative sanctions (*AMLA, Section 7(11)*) and cause the filing of criminal complaints with the Department of Justice ("DOJ") or the Ombudsman for the prosecution of money laundering offences (*AMLA, Section 7(4)*). The prosecution of money laundering criminal offences is handled by the DOJ and, with respect to money laundering criminal offences committed by public officers, and 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, Section 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 ranging anywhere from six months to fourteen 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, Section 14*). The court may also order the freezing, seizure and forfeiture of the assets which are the subject of a monetary laundering offence, or payment *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, governing the prescription of offences punished under special laws, shall be applicable. Depending on the act of money laundering committed and the corresponding imposable penalty, the prescription of offences under the AMLA will range from four to twelve years (*Act No. 3326, Section 1*).

1.8 Is enforcement only at the 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 tasked to seek 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 instrument 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, Section 12(a)*). Importantly, the petition for civil forfeiture shall proceed independently of the criminal prosecution (*A.M. No. 05-11-04, Section 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 its 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 its directors, officers, or employees has been convicted of the crime 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?

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 and its 2016 Revised Implementing Rules and Regulations ("IRR") 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 are:

- report to the AMLC 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;
- prohibit anonymous accounts, accounts under fictitious names, numbered accounts and all other similar accounts;
- keep records of all transactions for five years from the date of their occurrence;
- conduct customer due diligence based on a risk-based approach and maintain a system of verifying the true identity and legal existence of clients based on official documents, and updating the same;
- develop 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;
- observe ongoing monitoring of customers, accounts and transactions;
- register with AMLC's electronic reporting system;
- record identity of immediate family members and entities related to politically exposed persons;
- give to AMLC full access to all information pertaining to a transaction upon receipt of a bank inquiry order;
- formulate, implement and regularly update its money laundering prevention programme;
- provide training for officers and personnel;
- keep reports confidential; and
- for casinos, to: conform to high ethical standards and observe good corporate governance; 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 the 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? 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? If so, are the criteria for examination publicly available?

Yes. The AMLC functions as both the FIU and regulator of anti-money laundering laws in the Philippines.

The regulations relevant to AMLC's compliance monitoring are published on its website at http://www.amlc.gov.ph/laws/money-laundering/2016-revised-implementing-rules-and-regulations-of-republic-act-no-9160-as-amended.

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, Article 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 as may be determined by the AMLC to be appropriate, which shall not be more than PhP500,000 per violation. In no case shall the aggregate fine exceed 5% of the asset size of the violator (*AMLA, Section 14; AMLC Rules on the Imposition of Administrative Sanctions*).

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 for by the AMLC. Where a less serious violation was committed, a warning may suffice provided that it is a first time violation and corrective action was immediately taken. Where a serious violation was committed, a fine will not be imposed if it was a first offence, corrective action was immediately carried out, and no aggravating circumstance was 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, Sections 10 and 12*).

Additionally, public officials or employees who are found guilty of violations may suffer perpetual or temporary absolute disqualification from office.

Banks and other regulated financial institutions may also 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/civil in nature. Violations of anti-money laundering obligations are also subject to criminal sanctions (*AMLA, Section 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 checking 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 conducted. The administrative proceedings shall end upon the issuance of the Resolution by the AMLA. A motion for reconsideration may be filed upon the grounds provided by relevant laws. 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.

Under the IRR, 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, Section 3(a)(4) to 3(a)(7)*).

Casinos, including internet- and ship-based casinos operating within the territorial jurisdiction of the Philippines, with respect to their casino cash transactions related to their gaming operations, are also required to comply with anti-money laundering requirements.

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

Yes. The IRR mandates covered persons to maintain compliance programmes. Under Rule XVIII of the IRR, covered persons shall formulate and implement their money laundering prevention programme (MLPP) in accordance with the AMLA, the IRR, other AMLC issuances, and the anti-money laundering guidelines and circulars of their supervising regulatory authorities. The MLPP shall be approved by the responsible officer (for single proprietorship and partnership), the Board of Directors, the country or regional head, or its equivalent for local branches of foreign juridical entities.

Further, covered persons shall regularly update their MLPPs, in no case less frequently than every two years, to incorporate changes in anti-money laundering laws, rules and regulations, policies and procedures, latest trends in money laundering typologies, and latest guidelines and circulars of the supervising authorities. Training programmes shall also be provided to their employees and personnel.

The mandated programmes shall be made available upon request of the AMLC or the relevant supervising authorities.

3.3 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 Registration and Reporting Guidelines ("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, but 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.

3.4 Are there any requirements to report routine 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 3.8 below). Rule 9C(1) of the IRR states that covered persons shall ensure the accuracy and completeness of a covered transaction and suspicious transaction report, which shall be filed in the AMLC-prescribed forms and shall be submitted in electronic form and in a secured manner to the AMLC.

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

Yes. Under Rule IX-A of the IRR, in relation to cross-border correspondent banking and other similar relationships, 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 combating 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.

3.6 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 Rule IX 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 nature of the product, transaction or activity (*IRR, Rule IX*).

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.

3.7 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. The IRR provides that no shell bank shall be allowed to operate or be established in the Philippines. Covered persons shall refuse to deal, enter into, or continue a correspondent banking relationship with shell banks. They shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks (*IRR, Rule IX-A (3)*).

3.8 What is the criteria for reporting suspicious activity?

Transactions, regardless of the amount involved, are considered suspicious activity when any of the following circumstances exists:

- 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 institution;
- the transaction is in any way related to an unlawful activity or offence under the AMLA that is about to be, is being or has been committed; or
- any transaction that is similar or analogous to the foregoing.

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 and their employees are prohibited from directly or indirectly communicating, in any manner or by any means, to any person, entity, or media, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information related thereto.

3.9 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.

3.10 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 (*IRR, Rule IX-A(4)*).

For those not exceeding the threshold amount to be determined by the BSP or its equivalent in foreign currency, they shall include accurate and meaningful originator and beneficiary information. The following information shall remain with the transfer or related message through the payment chain:

- the name of the originator;
- the name of the beneficiary; and
- an account number of the originator and beneficiary, or, in its absence, a unique transaction reference number.

For those that are equal to or greater than the threshold amount or its equivalent in foreign currency, the following information shall be obtained from all qualifying wire transfers:

- the name of the originator;
- the originator account number where such an account is used to process the transaction;
- the originator's address, or national identity number, or customer identification number, or date and place of birth;
- the name of the beneficiary; and
- the beneficiary account number where such an account is used to process the transaction.

Should any wire/fund transfer amounting to or exceeding the threshold amount as determined by the BSP, or its equivalent in foreign currency, be unaccompanied by the required originator and beneficiary information, the beneficiary institution shall exert all efforts to establish the true and full identity and existence of the originator by requiring additional information from the originating institution or intermediary institution.

3.11 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. Rule IX-A(3) of the IRR states that a covered person dealing with bearer share entities shall be required to conduct enhanced due diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of

the account. 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.

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

None. The requirements stated in questions 3.3 and 3.8 are applicable to all covered persons, including non-financial institution businesses.

3.13 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 enumeration of covered persons to include money service business, trust companies, real estate developers, among others;
- add more unlawful activities (it is proposed that this term is replaced with "Predicate Offense");
- add provisions on retention of forfeited assets and cross-border declaration; and
- repeal 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 making the Philippines no longer subject to FATF's monitoring process 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, Counsel 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 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 Law Offices
3/F, 122 The Valero Tower
Valero Street, Salcedo Village
Makati City 1227
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 counselled 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 a recent decision dismissing 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 an adjunct professor at the University of the Philippines College of Law.

Louie Alfred G. Pantoni
Castillo Laman Tan Pantaleon
& San Jose Law Offices
5/F, 122 The Valero Tower
Valero Street, Salcedo Village
Makati City 1227
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 covers corporate and project finance, foreign investments, banking, securities, mergers and acquisitions, pharmaceutical law, corporate law, data privacy and competition law and intellectual property. He has worked on various mergers and acquisitions and financing transactions involving local and foreign clients.

He has 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 provisions.

CASTILLO LAMAN TAN
PANTALEON & SAN JOSE

Law Firm

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. Through the years, the firm has met the complex needs of clients in the rapidly-evolving Philippine environment by ensuring a high level of client involvement and professional legal expertise, encompassing a broad range of capabilities in practically every business area.

Portugal

Filipa Marques Júnior

Morais Leitão, Galvão Teles,
Soares da Silva & Associados, SP, RL.

Tiago Geraldo

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, 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 include tax evasion, incitement and exploitation of prostitution, child abuse, trafficking (arms, organs, drugs), bribery and corruption, influence peddling and any crime punishable with a minimum sentence above six months' imprisonment or with a maximum sentence above 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 by 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 competence 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 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 10 days of 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 the 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.

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.

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 the national level?

No, there are also requirements at the European Union level.

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

The government agencies and authorities responsible for examination for compliance and enforcement of 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. For other businesses, the same examination and enforcement is carried out by some professional associations and other government agencies and authorities.

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 statistic data related to suspicious transactions that have been reported and their results, and also data related to transnational information requests that have been sent, received or refused by FIU. You can find further information at the following link: http://www.portalbcft.pt/pt-pt/content/unidade-de-informa%C3%A7%C3%A3o-financeira.

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

In what concerns administrative 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 can reach a penalty of up to €5,000,000 depending on the nature of the entity, and may be aggravated up to double of the economic benefit obtained or up to 10% of the annual volume of business, in certain cases.

Penalty provisions concern: the illegitimate disclosure of information, communications, analyses or other elements, to clients or third parties; the disclosure or improper favouring of identity discovery of those who provided information, documents or elements concerning suspicious transactions; and the refusal of following orders or legitimate commands from sectorial authorities when given in the context of performing 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 administrative offences, besides monetary fines, additional sanctions such as: (i) losing for the State the object of the offence and the economic benefit obtained with the offence; (ii) closing 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) publishing the final or definitive decision.

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 concern illegitimate disclosure of information, disclosure and improper favouring of identity discovery and even disobedience.

There are also disciplinary 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 for assessment and collection of sanctions is carried out by several different government agencies and authorities, such as the Bank of Portugal, the Portuguese Securities Market Commission, the Portuguese Insurance and Pension Funds Supervisory Authority and even the General Inspectorate for Finance, 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. If the competent authority decides to impose a sanction on an individual or legal entity, they may appeal to a judicial court.

Not all resolutions of administrative penalty actions by competent authorities are public, because the publishing of the resolution must be decided by the competent authority as an additional sanction.

Yes, financial institutions have challenged penalty assessments in judicial and even administrative 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: credit, payment and electronic money institutions; investment firms and other financial companies; 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; securitisation companies; companies which commercialise contracts relating to the investment in tangible assets to the public; consultants for investment in securities; pension fund management companies; and 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 off-shore 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: providers of gambling, lottery or betting services, whether in an establishment or online; non-financial real estate entities; auditors, external accountants and tax advisors, whether as natural or legal persons; lawyers, solicitors, notaries and any other independent legal professionals performing certain activities; trust or company service providers in certain activities; other professionals who intervene in operations of selling and buying rights over professional sport's players; economic operators exercising auction or lending activities, economic operators importing or exporting rough diamonds; entities which are authorised to exercise the activity of transportation, custody, handling and distribution of funds and values; and other 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 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" in terms of accompanying internal control procedures regarding anti-money laundering and other risks. The Bank of Portugal defines several requirements for this "function" such as independence and adequacy.

3.3 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 made 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: the identification of the natural or legal persons involved, as well as any known information on their activity; the specific procedures of enquiry and analysis carried out; the characterising and descriptive elements of the operation; the specific suspicious factors identified by the entity; and a copy of all supporting documentation obtained by the entity during their 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 in compliance with a legal requirement, such as the reporting duty.

3.4 Are there any requirements to report routine 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 current anti-money laundering legislation allows for the ministry of justice to define certain types of transactions which should be systematically reported, as well as the layout, deadline, contents or other aspects of such reports. However, such regulation has not been passed at the present.

3.5 Are there cross-border transaction 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, regarding whether it is a national operation or a cross-border one. 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 a higher risk profile to the operation leading to enhanced due diligence measures having to be taken by the entities in question.

3.6 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 operation 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, when carrying out 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, whenever there is a suspicion of money laundering 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 justify it, information should be obtained regarding the origin and destination of the funds. There must be a constant monitoring of the business relationships in order to ensure that the operations carried out in its course are coherent 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. The Bank of Portugal is currently undergoing works for the issuance of additional regulation under Law 83/2017.

3.7 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?

Financial entities are prohibited 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.

3.8 What is the criteria for reporting suspicious activity?

If an entity knows, suspects or has enough reason to believe that certain funds or other assets, regardless of the amount involved, originated in criminal activity or are related to terrorism financing, they must report the suspicious activity.

3.9 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 19th November 2017. The register itself is still under implementation but its intention 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 in particular, to customer due diligence responsibilities.

3.10 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 characteristics of the operation.

But in the specific case of funds transfer when not associated with an account, the financial institution of the originator or the beneficiary must comply with collecting a certain amount of accurate information, depending on the type of the entity, and regarding the originator or beneficiary's identification, if the amount of the transfer is €15,000 or more (according to Regulation 5/2013 from the Bank of Portugal).

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

No, not since 2017.

3.12 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, considering there is a derogation of the reporting duty whenever the services provided for the client are in the context of a judicial process.

3.13 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. In that sense, there are anti-money laundering requirements applicable in terms of the information on beneficial ownership that needs to be collected from entities and 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?

The Bank of Portugal is preparing a regulatory instrument that was under public consultation until 29th March 2018. Other sectorial authorities are also preparing additional regulatory instruments.

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, Counsel of Europe (Moneyval) or IMF? If so, when was the last review?

FATF conducted an onsite visit (28th March–13th April 2017) and produced a Mutual Evaluation Report in December 2017, mentioned above. On 22nd April 2014, the IMF Report "Portugal: Eleventh Review Under the Extended Arrangement, and Request for Extension of the Arrangement and Waivers of Applicability of End-March Performance Criteria" was published that mentions AML efforts of Portugal.

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/pt-pt; however, it is not available in English. Some sectorial authorities may have internet pages in English, such as the Bank of Portugal (https://www.bportugal.pt/en/page/legislation-and-rules?mlid=1149) but usually the legislation is in Portuguese.

Filipa Marques Júnior
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Rua Castilho, 165
1070-050 Lisboa
Portugal

Tel: +351 213 817 400
Email: fmjunior@mlgts.pt
URL: www.mlgts.pt/en/

Filipa Marques Júnior joined the firm in 2002 and became a non-equity partner in 2016. She is a member of the litigation team and is active in the areas of criminal and regulatory litigation, investigations and compliance.

Filipa has assisted clients both in court proceedings and in the preventive and pre-litigation stages on matters relating to regulatory and criminal liability in the most diverse areas related to white-collar defence, such as anti-bribery and corruption, money laundering, tax crimes, market manipulation, and insider trading, among others. She also advises on criminal matters within the international judicial cooperation. In recent years Filipa has given special attention to developing preventive and compliance measures, working together with the clients on the prevention and investigation of possible wrongdoings. Filipa also conducts internal training on topics related to the prevention of corruption, money laundering and terrorism financing.

Former professor at the Law Faculty of Nova University, where she taught Interdisciplinary Legal Practice from 2008 to 2009.

Filipa was an advisor at the Legal Policy and Planning Office of the Ministry of Justice in the area of enforcement procedure from 2000 to 2001.

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 the area of 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 and founding associate of the Institute of Criminal Law and Criminal Studies 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.

MLGTS is a leading full-service law firm in Portugal, with a solid background of more than 80 years of experience.

Internationally recognised, its reputation stems from the excellence and high level of the services provided to clients, solid ethical values and a distinctive approach with cutting edge solutions.

Specialised legal services in the main areas of law and in different sectors of the economy are a benchmark of the firm leading to its involvement in the most important operations in Portugal, as well as in high value cross-border transactions and disputes.

With a team consisting of more than 200 lawyers, MLGTS has its head office in Lisbon and offices in Porto and Funchal (Madeira Island). To support clients' international strategies, MLGTS developed a network of associations with local firms in Angola, Mozambique and Macau (China) – MLGTS Legal Circle, which offers integrated multijurisdictional teams.

Key transactional practices

Administrative and Public Procurement, Banking and Finance, Capital Markets, Corporate and Commercial, European Law and Competition, Intellectual Property, Labour and Social Security, Litigation and Arbitration, Real Estate, Tax, Urban Planning and Environment.

Network memberships

MLGTS LEGAL CIRCLE – To address the needs of its clients throughout the world, particularly in Portuguese-speaking countries, MLGTS established solid associations and alliances with leading law firms in Angola, Macau (China) and Mozambique, creating MLGTS Legal Circle. While working in close cooperation, the member firms of the MLGTS Legal Circle combine local knowledge with the international experience and support of the whole network, enabling each firm to maximise the resources available to its clients.

LEX MUNDI – In 2001, MLGTS was admitted as the Portuguese member of Lex Mundi, the world's leading association of independent law firms. With more than 21,000 lawyers in 560 offices, Lex Mundi member firms are present in 100+ countries worldwide.

Other offices

Porto, Funchal, Angola, Macau (China), and Mozambique.

Russia

Rustam Kurmaev & Partners

Rustam Kurmaev

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.

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 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 the 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 back 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.

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 the 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? 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.

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.

Pursuant to Article 5 of Federal Law No. 115-FZ dated 1 August 2001 "On the Prevention of Criminal Proceeds Legalisation (Laundering) and Terrorist Financing", the requirements extend over the following organisations conducting activities with cash and other property:

- credit institutions;
- securities market professionals;
- insurance organisations (save for medical insurance organisations operating solely in the area of mandatory medical insurance), insurance brokers and leasing companies;
- organisations of the federal postal service;
- pawnshops;
- organisations trading in precious metals and stones, jewellery scrap precious metals, save for religious organisations, museums and organisations using precious metals for medical, scientific needs or as part of instruments;
- organisations keeping betting and gambling shops as well as companies organising lotteries, *pari mutuel* and other risk-based activities, including through electronic means;
- managing companies of investment funds, unit investments funds and non-public pension funds;
- organisations acting as intermediaries in transactions for the sale and purchase of real estate;
- payment processors;
- commercial organisations entering into factoring agreements as financial agents;
- consumer credit cooperatives, including agricultural consumer credit cooperatives;
- microfinance organisations;
- mutual insurance organisations;
- non-public state pensions funds holding a pensions insurance licence; and
- communications operators having the right to independently provide mobile telephone communication services, as well as communications operators having significant presence in the public network who have the right to independently provide data transmission services.

These organisations must request that their customers supply information on the origin of funds used for certain transactions, as well as inform the public authorities of suspicious transactions.

3.2 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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 transferred 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.

3.6 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 a 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.

3.7 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 a 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 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).

3.8 What is the criteria for reporting suspicious activity?

Information on transactions 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.

3.9 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 the beneficial owners of their customers.

3.10 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 the payee (names and taxpayer identification numbers). The bank will reject any payment order without such information.

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

The legislation does not currently allow for the issuance of bearer shares.

3.12 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; commercial organisations entering into factoring agreements as financial agents.

3.13 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, such requirements apply to organisations listed in question 3.1.

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, Counsel of Europe (Moneyval) or IMF? If so, when was the last review?

A system for combatting financial terrorism in the Russian Federation has been recognised as fully compliant with the international standards. The Financial Action Task Force (on Money Laundering) (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 & Partners
Presnenskaya nab, 8, bldg. 1
Moscow
Russia

Tel: +495 150 05 05
Email: Rustam.Kurmaev@rkplaw.ru
URL: https://rkplaw.ru/

Rustam Kurmaev specialises in the resolution of commercial disputes, as well as in the field of criminal and legal protection of business, systematically combining the comprehensive protection of executives and top managers of companies with the resolution of concomitant disputes for the company. Kurmaev has considerable experience representing interests of Russian and foreign companies in arbitration courts and courts of general jurisdiction, including the Supreme Arbitration Court and the Supreme Court. A lawyer is a universally recognised expert in the enforcement of judicial acts as prescribed by law procedures (enforcement proceedings and bankruptcy), and through the use of alternative tools. Kurmaev was declared the winner of Client Choice awards 2015–2016 in the category "Litigation in Russia". For many years he has been one of the recommended lawyers in dispute resolution according to the version of the leading international publications *The Legal 500* and *Chambers*, and also included in the list of the best lawyers in Russia in the field of judicial proceedings according to the study of the international legal guide *Best Lawyers 2012–2017*.

Рустам Курмаев | Партнеры

Rustam Kurmaev & Partners focuses on commercial litigation and dispute resolution, criminal law, white collar investigations, corporate conflicts, insolvency and bankruptcy proceedings and public law matters. Having represented prominent global companies and Russian giants on numerous big-ticket cases, the lawyers of the firm have built up a valued reputation for their pragmatic and effective approach, strategic thinking and the strength to get results when it matters the most. The lawyers and advocates on Rustam Kurmaev's team have experience in representing the interests of both global corporations, including Ikea, Volkswagen Group, Panasonic, Caterpillar, Gillette, Citibank, and Mars, and Russian market leaders – VimpelCom, 2x2 TV Channel, and Sberbank. "Rustam Kurmaev & Partners" have partners the UK, US and various regions of Russia. The fundamental principles of "Rustam Kurmaev & Partners" are a non-standard approach to any business and the commitment to achieving the goal with an intuitive knowledge of the business environment. Our team spares no effort to achieve results.

Singapore

Gary Low

Drew & Napier LLC

Vikram Ranjan Ramasamy

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 in his role as the Public Prosecutor ("**PP**") prosecutes money laundering offences 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 primary legislation targeting money laundering is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) ("**CDSA**"), in particular, sections 43, 44, 46, and 47. These provisions do not use the term "money laundering" *per se*.

What must be proven

Sections 43 and 44 of the CDSA deal with the offences of assisting another to retain the benefits of drug dealing, or from criminal conduct, respectively. Further, sections 46 and 47 of the CDSA deal with the offences of acquiring, possessing, using, concealing or transferring the benefits of drug dealing, or criminal conduct, respectively. The elements of these offences which the PP must prove are as follows:

Section	Physical element	Mental element
43 / 44	Entering into, or otherwise being concerned in an arrangement.	Knowing or having reasonable grounds to believe that by the arrangement: (a) the retention or control by or on behalf of another person of that other person's benefits of drug dealing / criminal conduct is facilitated (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise); or (b) that other person's benefits of drug dealing / from criminal conduct: (i) are used to secure funds that are placed at that other person's disposal, directly or indirectly; or (ii) are used for that other person's benefit to acquire property by way of investment or otherwise, and knowing or having reasonable grounds to believe that that other person is a person who carries on or has carried on drug dealing or has benefited from drug dealing / is a person who engages in or has engaged in criminal conduct or has benefited from criminal conduct.
46(1) / 47(1)	Conceal, disguise, convert, transfer, remove from the jurisdiction, acquire, possess, or use any property which is, or in whole or in part, directly or indirectly, represents, his benefits of drug dealing / from criminal conduct.	Strict liability.

Section	Physical element	Mental element
46(2) / 47(2)	Conceal, disguise, convert, transfer, or remove from the jurisdiction any such property described in the right column.	Knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits of drug dealing / from criminal conduct.
46(3) / 47(3)	Acquire, possess, or use any such property described in the right column.	Knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits of drug dealing / from criminal conduct.

In this regard, "drug dealing" means doing or being concerned in, whether in Singapore or elsewhere, any act constituting a drug dealing offence or a foreign drug dealing offence. Further, "criminal conduct" means doing or being concerned in, whether in Singapore or elsewhere, any act constituting a serious offence or a foreign serious offence (see section 2(1), CDSA).

Predicate offences

There are numerous predicate offences for money laundering.

The first category of predicate offences is "drug dealing offences", which means: (a) any of the offences specified in the First Schedule of the CDSA; (b) conspiracy, inciting another, or attempting to commit any of those offences; or (c) aiding, abetting, counselling or procuring the commission of any of those offences. In this regard, a "foreign drug dealing offence" means an offence against a corresponding law of a foreign country that consists of or includes conduct which, if the conduct had occurred in Singapore, would have constituted a drug dealing offence (see section 2(1), CDSA).

The second category of predicate offences is "serious offences", which means: (a) any of the offences specified in the Second Schedule of the CDSA; (b) conspiracy, inciting others, or attempting to commit any of those offences; or (c) aiding, abetting, counselling or procuring the commission of any of those offences. In this regard, a "foreign serious offence" means an offence (other than a foreign drug dealing offence) against the law of a foreign country or part thereof that consists of or includes conduct which, if the conduct had occurred in Singapore, would have constituted a serious offence, and includes a foreign serious tax offence (see section 2(1), CDSA).

Tax evasion under Singapore law and the national law of a foreign country in certain specified forms constitutes a serious offence and a foreign serious tax offence, respectively (and hence are predicate offences), for the money laundering offences under sections 44 and 47 of the CDSA (see section 2(1) and the Second Schedule, CDSA).

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

Yes, the CDSA can apply whether the predicate offences take place in Singapore or elsewhere (see question 1.2 above).

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

The primary investigative agency for money laundering offences is the Commercial Affairs Department ("**CAD**"), a department of the Singapore Police Force ("**SPF**"). Officers of the Central Narcotics Bureau and the Corrupt Practices Investigation Bureau are also involved in investigating certain kinds of money laundering offences. The CDSA expressly confers officers of these agencies with various powers and rights to aid in their investigation of money laundering offences.

The PP and the officers of the Attorney-General's Chambers ("**AGC**") acting under the authority of the PP prosecute money laundering offences in consultation with the aforementioned investigative agencies.

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

There is both corporate criminal liability and liability for natural persons under the CDSA.

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

The maximum penalties for an offence under sections 43, 44, 46, and 47 of the CDSA are: (a) if the person is an individual, a fine not exceeding S$500,000 or imprisonment for a term not exceeding 10 years or both, per charge; and (b) if the person is not an individual, a fine not exceeding S$1,000,000, per charge.

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

There is no applicable limitation period for money laundering crimes or for the prosecution of criminal offences in general. Nevertheless, where there has been an inordinate delay in prosecution, this may be a factor that the Court considers in sentencing.

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

Yes, enforcement is only at national level. There is no "state" or "provincial" criminal legislation, as there are no states or provinces in Singapore.

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.

Under section 2(1) of the CDSA, "property" is defined broadly to mean money and all other property, movable or immovable, including things in action and other intangible or incorporeal property. Pursuant to sections 4 and 5 of the CDSA, where a defendant is convicted of one or more drug dealing offences or

serious offences, the Court shall, on the application of the PP, make a confiscation order against the defendant in respect of benefits derived by him from drug dealing or criminal conduct if the Court is satisfied that such benefits have been so derived.

Under the Organised Crime Act 2015 (No. 26 of 2015) ("**OCA**"), the PP may apply to the Court for a confiscation order and the Court is to make such an order against a person if it is satisfied on a balance of probabilities that the said person has: (a) carried out organised crime activity (including the offences under sections 43, 44, 46, and 47 of the CDSA) within the defined statutory period; and (b) derived benefits from the organised crime activity (see sections 61(1) and 61(2), OCA). Crucially, the organised crime activity on which the said confiscation order is based does not need to be, or to have been, the subject of any criminal proceedings (see section 51, OCA). Further, if criminal proceedings are instituted or pending or have been discontinued or determined in respect of any organised crime activity that is the basis for a confiscation order made under the OCA, the said confiscation order is not affected by the criminal proceedings, even if the person is acquitted (see section 53, OCA). In this regard, "property" is defined in the same way under the OCA as the CDSA (see section 2(1), OCA).

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

While it is rare for banks and other regulated financial institutions ("**FIs**") to be formally charged and convicted in Court for money laundering offences, officers and employees of FIs have previously been convicted in Court for such offences in Singapore. For example, in July 2017, one Yeo Jiawei, a former wealth planner at BSI Bank Limited ("**BSI**"), was sentenced to 54 months' imprisonment for money laundering and cheating in a case related to the probe into 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 under the CDSA are generally resolved through the judicial process.

However, following the passage of the Criminal Justice Reform Bill on 19 March 2018, certain specified criminal actions (including those in respect of offences under sections 43, 44, 46, and 47 of the CDSA) may now be resolved through deferred prosecution agreements ("**DPAs**"). A DPA comes into force only when the High Court approves it by making a declaration that the DPA is in the interests of justice, and that its terms are fair, reasonable, and proportionate. After such approval, the DPA must in general be published.

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**") is the integrated financial regulator that imposes anti-money laundering ("**AML**") requirements on FIs in Singapore. Other authorities / agencies that impose AML requirements on designated non-financial businesses and professions ("**DNFBPs**") include the Casino Regulatory Authority of Singapore (for casino operators), the Accounting and Corporate Regulatory Authority ("**ACRA**") (for corporate service providers, public accountants and accounting entities), and the Council for Estate Agencies (for estate agents and salespersons). In respect of the details of the said AML requirements, see question 3.1 below.

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

Yes, there are self-regulatory organisations and professional associations that impose AML requirements on various DNFBPs, including the Council of the Law Society of Singapore (for legal practitioners and law practices) and the Council of the Institute of Singapore Chartered Accountants (for professional accountants and professional accounting firms).

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

Yes, self-regulatory organisations and professional associations play a role in ensuring AML compliance and may have their own enforcement measures against errant members.

For example, for legal practitioners and law practices, contravention of the provisions of the Legal Profession Act (Cap. 161) ("**LPA**") (read with the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015) relating to, among other things, AML, may subject the offending legal practitioner or law practice to disciplinary proceedings or regulatory actions under the LPA.

2.4 Are there requirements only at the 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? Are the criteria for examination publicly available?

The Suspicious Transaction Reporting Office ("**STRO**") and the agencies set out at question 1.4 above are responsible for the examination for compliance (see question 2.6 below) and enforcement of AML requirements under the CDSA, respectively.

Separately, MAS is Singapore's integrated financial regulator, while various other government authorities / agencies are responsible for the examination for compliance and enforcement of AML requirements in specific industry sectors (see question 2.1 above). Further, the Registrar of Moneylenders and the Registrar of Pawnbrokers oversee the regulation of moneylenders and pawnbrokers in Singapore, respectively.

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?

The STRO is Singapore's FIU. It receives Suspicious Transaction

Reports ("**STRs**") and other financial information, including Cash Transaction Reports ("**CTRs**"), and Physical Currency and Bearer Negotiable Instruments Reports ("**CBNI Reports**") (in respect of cross-border movements of physical currency and bearer negotiable instruments ("**CBNI**")), and analyses such information to detect, among other things, money laundering offences. Thereafter, the STRO disseminates the results of any such analysis to the relevant regulatory and enforcement authorities / agencies.

Industry sector regulators may also issue directions and guidelines on AML measures, including the manner of suspicious transaction reporting, as well as the types of suspicious transactions that each industry should take note of. These are typically issued with input from the STRO and are usually publicly available.

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

There is no applicable limitation period 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?

The penalties for failure to comply with the relevant regulatory / administrative AML requirements vary across industry sectors.

In the case of FIs, under the Monetary Authority of Singapore Act (Cap. 186) ("**MAS Act**"), where a FI is convicted for failing to comply with or contravening any direction issued or regulation made by MAS for the prevention of money laundering, it is liable to a fine not exceeding S$1,000,000, per charge, and, in the case of a continuing offence, to a further fine of S$100,000 for every day or part of a day during which the offence continues after conviction, per charge (see section 27B(2), MAS Act).

In practice, non-compliance with AML requirements may be compounded into financial settlements without criminal prosecution. In this regard, MAS has the discretion to compound any offence under the MAS Act which is punishable with a fine only by collecting from a person reasonably suspected of having committed the offence a sum of money not exceeding one-half of the amount of the maximum fine prescribed for that offence (see section 41A(1), MAS Act, and regulation 2, Monetary Authority of Singapore (Composition of Offences) Regulations 2007). Apart from financial penalties, MAS has other sanctions at its disposal (see question 2.9 below).

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

Again, sanctions vary across industry sectors. In the case of FIs, MAS can impose non-financial sanctions such as formal warnings / reprimands, prohibition orders against culpable individuals, placing restrictions on operations, and even revoking licences. For example, in 2016, following investigations into 1MDB, MAS withdrew the merchant bank status of BSI and Falcon Private Bank Ltd, Singapore Branch for, among other things, serious breaches of AML requirements.

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

Violations of AML obligations are also subject to criminal sanctions in certain instances. For example, under section 27B(2) of the MAS Act, it is an offence if a FI fails to comply with or contravenes any AML direction issued or regulation made by MAS (see question 2.8 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?

In general, the relevant regulatory authority will assess the appropriate sanction(s) to be imposed based on its own internal guidelines and precedents. Judicial review of administrative decisions is possible, but rarely pursued in practice. Typically, most resolutions of penalty actions are published by the relevant regulatory authority. As penalty assessments are usually composition fines, FIs cannot, by the nature of the composition of offences, challenge them.

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 FIs and DNFBPs are subject to specific AML requirements in addition to those under the CDSA:

(a) FIs: approved trustees of a collective investment scheme authorised under the Securities and Futures Act (Cap. 289), banks, capital markets intermediaries, credit card or charge card licensees, direct life insurers, financial advisers, finance companies, insurance brokers, merchant banks, money-changing or remittance business licensees, stored value facility holders, The Central Depository (Pte) Limited ("**CDP**"), and trust companies; and

(b) DNFBPs: casino operators, corporate service providers, dealers in precious stones and / or precious metals, 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 obligations of the said FIs and DNFBPs are set out in specific statutes, subsidiary legislation, directions, guidelines, codes, and practice notes / circulars. These typically include: (i) undertaking customer due diligence ("**CDD**") measures; (ii) reporting requirements; (iii) record keeping requirements; and (iv) developing and implementing internal policies, procedures, and controls. In doing so, a risk-based approach is commonly adopted to identify, assess, manage, and mitigate money laundering risks.

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

Again, these vary across industry sectors, but FIs and DNFBPs subject to AML requirements are generally required to have a basic compliance framework in place. This will typically include measures in relation to CDD, reporting, record keeping, and internal policies, procedures, and controls (see question 3.1 above).

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

Record keeping

Requirements for record keeping vary across industry sectors. FIs and DNFBPs subject to AML requirements are required to retain CDD, transaction, and other relevant documents and information for a minimum period of generally five years.

Further, under the CDSA, FIs must retain and store financial transaction documents for a minimum period of five years (see sections 36 and 37, CDSA).

Reporting large currency transactions

A dealer in precious stones and / or precious metals who enters into any of the following cash transactions must submit a CTR relating to that transaction to the STRO:

(a) a single cash transaction with a customer the value of which exceeds S$20,000 (or its equivalent in a foreign currency); or

(b) two or more cash transactions in a single day with the same customer, or with customers whom the said dealer knows act on behalf of the same person, the total value of which exceeds S$20,000 (or its equivalent in a foreign currency).

The CTR must be submitted within 15 business days after the date on which the cash transaction is entered into (in the case of (a)), or all of those cash transactions are entered into (in the case of (b)) (see sections 48H, 48I and 48J, CDSA, and regulations 4, 7, and 10, Corruption, Drug Trafficking and Other Serious Crimes (Cash Transaction Reports) Regulations 2014). Further, such dealers must maintain records of such cash transactions, as well as customer information, for a period of five years (see section 48K, CDSA).

Similarly, a casino operator must file with the STRO a CTR of: (a) every cash transaction with a patron involving either cash in or cash out of S$10,000 or more in a single transaction, within 15 days after the date on which the single cash transaction takes place; or (b) multiple cash transactions which the casino operator knows are entered into by or on behalf of a patron, the aggregate of which is either cash in or cash out of S$10,000 or more in any gaming day, within 15 days after the date the last transaction of the multiple cash transactions takes place (see regulation 3, Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009).

For when a CBNI Report must be filed in respect of cross-border movements of CBNI, see question 3.5 below.

3.4 Are there any requirements to report routine 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 CBNI Reports are the other types of reports that may be filed with the STRO. For when a STR must be filed, see question 3.8 below. For when a CBNI Report must be filed, see question 3.5 below.

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

Yes, a person who moves or attempts to move into or out of Singapore CBNI the total value of which exceeds S$20,000 (or its equivalent in a foreign currency), must give a report in respect of the movement. Further, a person who receives CBNI the total value of which exceeds S$20,000 (or its equivalent in a foreign currency), which is moved to the person from outside Singapore, must make a report in respect of the receipt within five business days beginning on the day of the receipt (see 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).

The CDSA provides for exemptions from the first reporting requirement above (see sections 48C(7) and 48C(8), CDSA). Further exemptions in respect of both reporting requirements above are set out in the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) (Exemption) Orders 2007 and 2010.

3.6 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 identification and CDD requirements for FIs and DNFBPs subject to AML requirements commonly 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.

As mentioned in question 3.1 above, a risk-based approach is commonly adopted. Therefore, enhanced CDD measures are required for certain types of customers / transactions where the risk of money laundering is higher, including where the relevant FI or DNFBP is dealing with a politically-exposed person (or a family member or close associate of a politically-exposed person), or where a customer is from or in, or the transaction relates to, a country or jurisdiction in relation to which the Financial Action Task Force ("**FATF**") has called for countermeasures or enhanced CDD measures, or is known to have inadequate AML measures. Such enhanced CDD measures commonly include obtaining the approval of senior management before establishing or continuing a business relationship with the customer, taking reasonable measures to establish the customer's source of wealth / funds, and conducting enhanced ongoing monitoring of the business relationship with the customer.

3.7 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 entering into or continuing correspondent banking or other similar services relationship (in the case of banks, finance companies, and merchant banks) / correspondent account services relationship (in the case of capital markets intermediaries) / correspondent account relations (in the case of the CDP) / correspondent account services or other similar services relationship (in the case of stored value facility holders) with shell FIs, and each must take appropriate measures when establishing the relevant relationship, to satisfy itself that its respondent FIs do not permit their accounts to be used by shell FIs.

The provision of remittance services to shell FIs by money-changing or remittance business licensees is also prohibited (see paragraph 10.5 of MAS Notice 3001).

3.8 What is the criteria for reporting suspicious activity?

If a person knows or has reasonable grounds to suspect that any property: (a) in whole or in part, directly or indirectly, represents the proceeds of; (b) was used in connection with; or (c) is intended to be used in connection with, any act which may constitute drug dealing / criminal conduct, and 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, then he must make a STR disclosing the knowledge or suspicion or the information or other matter on which that knowledge or suspicion is based as soon as is reasonably practicable after it comes to his attention (see section 39, CDSA).

3.9 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?

ACRA maintains a 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. Such information includes particulars of management (directors of the company, or sole proprietor, or partners), 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). Business profiles of entities are publicly available online for purchase to assist FIs and DNFBPs with their AML CDD responsibilities.

3.10 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 a requirement that accurate information about originators and beneficiaries be included in the message or payment instruction that accompanies or relates to a wire transfer. 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, paragraph 11 of MAS Notice 824, paragraph 11 of MAS Notice 1014, and paragraph 12 of MAS Notice 3001).

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

Ownership of legal entities in the form of bearer shares is not permitted in Singapore (see sections 66 and 364, Companies Act (Cap. 50)).

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

Yes, specific AML requirements are applicable to non-FI businesses (i.e. DNFBPs) (see questions 3.1, 3.3, and 3.6 above).

3.13 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, see questions 3.1 to 3.3, 3.6, 3.7 and 3.10 above.

4 General

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

Singapore is committed to continuously bolstering its AML framework. For example, MAS recently issued a Consultation Paper on 16 January 2018, inviting comments from stakeholders on proposed enhancements to AML requirements for the money-changing and remittance business sector. Specifically, MAS proposes to: (a) issue a new notice that would prohibit issuance of bearer instruments and restrict cash pay-outs of S$20,000 and above (or such equivalent amount in foreign currency); and (b) amend MAS Notice 3001 to facilitate non-face-to-face business and better mitigate the money laundering risks of foreign exchange transactions.

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 review, Singapore was rated at least partially compliant for each of the FATF 40 Recommendations (see FATF and Asia/Pacific Group on Money Laundering's ("**APG**") Mutual Evaluation Report (September 2016), accessible at: http://www.fatf-gafi.org/countries/s-t/singapore/documents/mer-singapore-2016.html).

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

Yes, Singapore's AML regime was subject to evaluation by FATF and APG in late 2015 (see 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?

Relevant materials (in English) on AML laws, regulations, administrative decisions, and guidance can be obtained from various websites, especially MAS's website (http://www.mas.gov.sg), SPF's website (http://www.police.gov.sg), and Singapore Statutes Online (http://sso.agc.gov.sg/).

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Priya Gobal and Chan Min Jian in preparing this chapter.

Gary Low
Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 2497
Email: gary.low@drewnapier.com
URL: www.drewnapier.com

Gary practises both civil and criminal litigation. He has an active civil/commercial practice and has acted in a wide variety of matters, including disputes in banking and finance, commercial disputes, arbitrations, directors'/shareholders' disputes, minority oppression, tortious liability, property and contractual disputes. Additionally, he has also represented clients for commercial crimes, corruption and securities offences such as insider trading and market manipulation. He has also advised on anti-money laundering practices and been involved in investigations by various corporations into alleged wrongdoings of employees in relation to fraud, criminal breach of trust, cheating, breach of fiduciary duties and other misconduct. Gary is recommended by name in the most recent edition of the *Asia Pacific Legal 500* (Dispute Resolution) and is listed in *Who's Who Legal* (Business Crime Defence – Corporates).

Vikram Ranjan Ramasamy
Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 2408
Email: vikram.ranjan@drewnapier.com
URL: www.drewnapier.com

Vikram has acted in a wide range of civil matters. He has advised and represented local and international clients at all levels of the Singapore Courts in respect of diverse corporate and commercial disputes relating to, among other things, commercial contracts, banking and finance, employment matters, engineering and construction projects, trusts, wills and probate, real estate matters, and tortious liability. He has also advised and acted for clients in a variety of criminal offences, including criminal breach of trust, corruption, cheating, and non-commercial crime. Vikram has also been engaged by various corporate entities to investigate and advise on alleged wrongdoings by employees and their potential criminal liability.

DREW & NAPIER

Drew & Napier has been providing exceptional legal service and representation to discerning clients since 1889. We are one of the largest law firms in Singapore. The calibre of our work is acknowledged internationally at the highest levels of government and industry, and marks us as Singapore's world class law firm.

Drew & Napier's Criminal Practice comprises an exceptional team of specialists from across the firm's practice groups including Banking & Corporate, Tax, Intellectual Property, and Dispute Resolution. We provide our clients with a single access point for representation on commercial, securities, and non-commercial crimes. Our lawyers have dealt with an extensive range of criminal matters and we have experience in regulatory, trial, and appeal processes. We are committed to providing support for our clients at every stage of the criminal justice process from investigations to prosecutions in court. Our clients include major corporations, listed companies, and individuals.

Chapter 29

Switzerland

Omar Abo Youssef

Lea Ruckstuhl

Kellerhals Carrard Zürich KlG

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. 51 para. 1 of the Federal Act on the Swiss Financial Market Supervisory Authority [FINMASA]). For more details about the reporting obligation we refer to question 3.8.

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 the national level? Are there parallel state or provincial criminal offences?

Yes. 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 (for example, 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. On 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 the sum of EUR 5 million to an account at the bank – the transfer was based on fraud – CHF 4.6 million were 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 combating 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 3.6 for the requirements related to combating 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 the 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? 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 don't 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 3.6 for a description of the due diligence obligations.

3.2 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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).

3.7 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.

3.8 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).

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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 recently 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.

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, Counsel 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 eleven 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/19370083/index.html.

Anti-Money Laundering Act, AMLA:

https://www.admin.ch/opc/en/classified-compilation/19970427/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 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 Zürich KlG
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 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 Zürich KlG
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 Zürich KlG since 2011.

Thanks to her job 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 combating 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.

Kellerhals Carrard

With 160 professionals (comprised of partners, salaried lawyers, legal experts, tax advisers and notaries) and a total of more than 260 staff, the law firm Kellerhals Carrard, which dates back to 1885 and has offices in Basel, Berne, Lausanne, Lugano, Sion and Zurich and representation offices in Binningen and Shanghai, is one of the 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 White Collar Crime team consists of 15 lawyers.

Turkey

EB LEGAL

Prof. Av. Esra Bicen

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 autonomous offence defined under Article 282 of the Turkish Criminal Law (Law No. 5237 "TCL"). Turkey ratified the United Nations (UN) Convention Against Transnational Organized Crime ("Palermo Convention") into law on 30 January 2003 and has since largely implemented the definition of a money laundering offence from the Palermo Convention into Article 282 of TCL. Article 282 of TCL defines a money laundering offence as follows:

ARTICLE 282: (...)

> *(1) A person who transfers abroad the proceeds obtained from an offence requiring a minimum penalty of six months or more imprisonment or processes such proceeds in various ways in order to conceal the illicit source of such proceeds or to give the impression that they have been legitimately acquired shall be sentenced to imprisonment from three years up to seven years and a judicial fine up to twenty thousand days.*
>
> *(2) A person, who without participating in the commitment of the offence mentioned in paragraph (1), purchases, accepts, possesses or uses the proceeds, which is the subject of that offence knowing the nature of the proceeds shall be sentenced to imprisonment from two years up to five years.*

Criminal enforcement at national level rests with public prosecutors and governed by Criminal Procedure Law (Law No. 5320 "CPL").

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?

Pursuant to Article 21 of TCL, the government must prove the intent of the perpetrator. Intent means carrying out the elements of a crime knowingly and wilfully. Based on the definition of the money laundering offence, as for the first element of this crime, it should be proven that "*it was known that the proceeds being transferred abroad were derived from a crime*". As for the second element of the offence, intent to "*disguise illicit sources*" and "*give the impression that they seem to be derived from legitimate sources*" should be proven. Article 282 of TCL does not, however, require that the perpetrator be convicted of a predicate offence in order to prosecute a money laundering offence.

The old TCL had adopted the listing approach for money laundering offences, which was partly compliant with the Designated Category of offences in the FATF 40 Recommendations. The new TCL 5237 replaced the "*listing*" approach with the "*minimum threshold*" approach and greatly exceeded the number of predicate offences listed in FATF recommendations by defining such offences as all crimes punishable with a minimum imprisonment term of six months. Under Article 282 of TCL, predicate offences for prosecuting money laundering offences in Turkey consist of:

- Terrorism and terrorist financing.
- Participation in an organised criminal group and racketeering.
- Human trafficking and migrant smuggling.
- Organ trafficking.
- Illicit trafficking of narcotic drugs and controlled substances.
- Illicit arms trafficking.
- Murder and grievous bodily injury.
- Sexual exploitation, exploitation of children.
- Kidnapping, illegal restraint, hostage taking.
- Robbery, theft.
- Opposition to data privacy laws.
- Fraud, bankruptcy fraud.
- Banking crimes under Banking Law No. 5411 (i.e. unauthorised banking activity, defrauding depositors and participation fund holders, failure to implement remedial and restrictive measures, failure to cooperate with regulatory authorities, failure to comply with record keeping and privacy laws, out of book transactions and false accounting).
- Tax evasion under Tax Procedure Law No. 213 (i.e. accounting and bookkeeping fraud, opening fictitious bank accounts, destroying and concealing accounting records, falsifying figures in books and accounts, forging books, records and certificates).
- Providing false information regarding a corporation or cooperative.
- Environmental pollution.
- Nutrient pollution and contamination of drinking water.
- Forgery, including counterfeiting money, valuable seals belonging to the state, public documents, precious metals.
- Piracy.
- Insider trading and market manipulation.
- Providing a venue or means for gambling.
- Public procurement fraud.
- Price fixing, manipulating employee benefits and other anti-competitive behaviour.
- Cyber-attack.

- Embezzlement, bribery, corruption.
- False testimony, perjury, obstruction of justice, tampering with evidence.
- Opposition to sovereignty of state, constitutional order or national security.

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

Yes. Perpetrators shall be prosecuted for money laundering offences carried out in Turkey involving proceeds of predicate crimes committed in foreign countries. Conviction for the predicate offence committed abroad is not required. However dual criminality for the predicate offence is required. In addition, under Articles 11 to 13 of TCL, Turkish criminal courts have jurisdiction over serious crimes (with a minimum prison term of one year) committed abroad.

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

Under CPL, prosecution of any offence rests with the public prosecutors. Public prosecutors are responsible for conducting investigations and initiating criminal lawsuits related to money laundering. Prosecutors conduct investigations and prosecutions either directly through their law enforcement units or indirectly through the General Directorate of Turkish National Police, General Command of Gendarmerie, Undersecretariate of Customs, Ministry of Interior's General Directorate of Security or General Command of Coast Guard. Under Articles 123-134 of CPL, judges and, if time is of the essence, pending a final court decision, prosecutors may order decisions to confiscate goods and proceeds derived from criminal activity.

The Ministry of Interior's General Directorate of Security has two dedicated departments; namely, the Department of Anti-Smuggling and Organized Crime and Anti-Terror and Intelligence for investigating AML offences. The Anti-Smuggling Department is responsible for combatting serious financial fraud and corruption whereas the Anti-Terror Department is responsible for combatting all kinds of smuggling. The Undersecretariate of Customs, through its customs enforcement units, is responsible for cross-border movement of cash and valuables and combatting all kinds of smuggling.

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

Article 20 of TCL provides that criminal liability is personal and that it does not apply to legal persons. It further states that where an offence is committed for the benefit of a legal person, security measures (*koruma tedbirleri*) will apply to such legal persons. Article 60 of TCL lists security measures as cancellation of a licence or permit, seizure and confiscation of goods and proceeds derived from criminal activities.

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

The perpetrator of a money laundering offence shall be subject to imprisonment from three to seven years and a judicial fine up to 20,000 days. Perpetrators who knowingly purchase, accept, possess or use proceeds of a money laundering crime shall be subject to imprisonment from two years to five years. Where the offence is committed by public servants or professionals, the penalty is increased by one half. If an AML offence is committed by a criminal organisation, the penalty is increased two-fold. Legal entities will be subject to security measures.

Those who assist legal authorities in locating the proceeds of money laundering offences prior to initiation of criminal proceedings (during prosecution stage) will not be penalised.

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

The statute of limitations for initiating criminal proceedings is eight years for offences subject to sanctions of imprisonment of up to five years and judicial fines and 15 years for offences subject to sanctions of imprisonment from five to 20 years.

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

Enforcement is 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?

Turkey does not have a civil forfeiture system. Articles 54 and 55 of CPL allow for the confiscation of property and material benefits that are subject of, or derived from, a criminal activity together with any economic proceeds obtained through their conversion. TCL does not require conviction for the predicate offence in order to render a confiscation order. In cases where the property has been used, transferred to third parties acquiring it in good faith or consumed, its equivalent value will be confiscated.

Pursuant to Article 128 of CPL, property or funds derived from a criminal activity can be confiscated by means of a decision of a criminal judge, where there is strong suspicion that a crime subject to investigation or prosecution has been committed. In circumstances where delay may hinder proceedings, the public prosecutor may issue a seizure order, which must be approved by the criminal judge within 24 hours. Failing to obtain court approval would render such seizure order void.

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

No, they have not.

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?

Article 253 of CPL lists certain offences and allows for settlement (*uzlasma*) as an out of court dispute resolution procedure. These offences may be resolved through negotiations held between the perpetrator/s and the mediator before the Bureau of Settlement (*Uzlastirma Burosu*) located in the jurisdiction of the office of the public prosecutor. Settlement negotiations are confidential

and settlement reports and relevant evidence are submitted to the office of the public prosecutor to be kept in the investigation file. Declarations made during settlement negotiations are not considered admissible evidence in the pending investigation or judicial proceedings. Money laundering is not listed among the offences subject to settlement.

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.

Legal authorities imposing anti-money laundering ("AML") requirements are:

- Law on Prevention of Laundering Proceeds of Crime (Law No. 5549 "AML Law") effective since 18 October 2006.
- Regulation on Measures regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("ROM") effective since 1 April 2008.
- Regulation on the Program of Compliance with Obligations of Anti-Money Laundering and Combatting the Financing of Terrorism ("ROC"), effective since 1 October 2008.
- MASAK Communiqués on preventive measures and MASAK Guidelines on Suspicious Transaction Reporting of August 2016 concerning suspicious transaction reporting (Financial Crimes Investigation Board – Mali Suclari Arastirma Kurulu "MASAK" is the financial intelligence unit of Turkey).

AML Law sets forth preventive measures applicable to financial institutions and other businesses. Two regulations, ROM and ROC, were adopted for the implementation of the AML Law. ROM applies to all natural and legal persons defined under the AML Law. ROC only applies to banks, brokerage houses, insurance and pension companies and postal administration.

Preventive measures under AML legislation cover requirements of customer identification for different types of customers, reporting of suspicious transactions, implementing institutional policies and internal compliance, establishing monitoring and controls, regulating correspondence relationships, wire transfers, disclosures to authorities, record keeping and mutual legal cooperation with other countries.

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

MASAK is the sole self-regulatory body ("SRO") imposing AML requirements in the form of Communiqués and Guidelines upon the financial sector and other businesses. MASAK Communiqué Nos. 1-5 and 6 have been repealed. MASAK Communiqué No. 5 addresses customer identification requirements involving different kinds of customers and transactions by various risk categories. Communiqué No. 7 relates to customer identification and applies to ongoing business relations and natural persons. Communiqué No. 8 extends the period for obliged persons to comply with customer ID requirements. Communiqué No. 9 amends No. 5 with respect to specified customers such as banks, international organisations, diplomatic agencies and transactions involving pension plans and life insurance plans. Communiqué No. 13 sets forth procedures of suspicious transaction reporting.

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

Yes. Self-regulating organisations such as MASAK, the Banking Regulatory and Supervision Agency (BRSA), the Capital Markets Board (CMB) and the Undersecretariate of Treasury (UT) are responsible for supervision of the implementation of laws and regulations. The Undersecretariate of the Treasury is responsible for supervising activities of bureaux de change, insurance companies, money lenders and precious metals exchange institutions. SROs are authorised under the AML Law, Banking Law (Law No. 5411) and Capital Markets Law (Law No. 2499) to inspect compliance of financial institutions with AML requirements, to obtain information and documents and to report any violation to MASAK.

2.4 Are there requirements only at the national level?

No. AML Law provides that the AML requirements established for obliged persons will also apply to their agents, branches, commercial representatives or similar affiliated units located abroad to the extent allowed by the laws of the foreign jurisdiction.

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

Article 19 of AML Law authorises MASAK to examine compliance of obliged persons with AML requirements. MASAK utilises inspectors from other government agencies such as the Ministry of Finance, Ministry of Interior, Ministry of Justice, Undersecretariate of Treasury and Undersecretariate of Customs to carry out AML compliance examinations. AML examinations are conducted either upon MASAK's own initiative or by a request of the public prosecutor from MASAK. MASAK assigns examination duty to inspectors from various government agencies; i.e. tax inspectors, auditors, revenue comptrollers, customs inspectors, treasury comptrollers, insurance auditors and actuaries, BRSA and CMB specialists.

Article 7 of AML Law authorises inspectors to demand access to all information and documents relevant to the examination from public and private financial institutions, natural and legal persons and non-profit organisations. Any violations detected must be reported to MASAK. MASAK would then inform the public prosecutors to initiate judicial proceedings. Sanctions for violation of AML laws and regulations shall be applied by the courts.

The legal basis for AML requirements are set forth in the AML Law and its secondary legislation, ROC, ROM and MASAK Communiqués. Examinations are conducted by checking compliance with the AML requirements that are applicable to obliged persons. In addition, MASAK issues sectoral guidelines providing explanations as to specific AML requirements such as STR Guidelines of 2016, Guidelines on Examination of Compliance and Guidelines for Investigating Money Laundering Crimes. MASAK published a manual for inspectors on conducting examinations of money laundering crimes. MASAK also organises education and training programmes for the financial sector and law enforcement units.

MASAK publishes its annual activity reports on its website, which include statistics on suspicious transaction reports, judicial investigations and results of AML cases.

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?

MASAK is the financial intelligence unit of Turkey. MASAK directly reports to the Minister of Finance. Article 19 of AML Law gives MASAK the following powers:

- to collect information, documents and records from obliged parties, to evaluate and analyse reported information, to exchange information with FIUs of foreign countries, sign memoranda of understanding for mutual cooperation with foreign FIUs;
- to develop policy, prepare draft laws, communiqués and guidelines, to organise public activities to increase awareness of AML requirements;
- to coordinate through joint activities and reviews with other government agencies and institutions to implement regulations;
- to supervise compliance of obliged persons with AML requirements; and
- to carry out investigations directly through MASAK inspectors or by requesting inspection personnel from other agencies, to collect information data and documents, to review data and suspicious transaction reports submitted, to initiate judicial proceedings by involving public prosecutors and other law enforcement units.

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

Under CPL, the statute of limitation for enforcement is 10 years for imprisonment up to five years and judicial fines, and 20 years for imprisonment from five to 20 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?

As of 2018, the AML Law imposes an administrative fine of TL 12,152 upon the obliged party for violations of Articles 3 (customer identification), 4(1) (suspicious transaction reporting), 5 (training and internal control and risk management systems) and 6 (periodical reporting of transactions exceeding a determined threshold) of the AML Law. In case the obliged party is a financial institution, the penalty can be doubled; i.e. TL 24,304. The annual cap for administrative fines is TL 13,817,280 for financial institutions and TL 1,381,720 for other obliged parties.

Violation of the electronic service requirement shall be subject to an administrative fine of TL 13,816 with an annual upper limit of TL 354,420.

Failure to provide accurate information to the Customs authorities regarding Turkish currency, foreign currency or instruments ensuring payment shall be subject to an administrative fine equivalent to 1/10th of the undisclosed monetary value.

The AML Law imposes a judicial fine of up to 5,000 days for violation of Articles 4(2) (tipping off information regarding an investigation), 7 (failure to provide information, documents and records to MASAK or the inspectors) and 8 (record keeping) of the AML Law.

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

Security measures apply to legal persons for violations of AML requirements imposing a judicial fine. Security measures involve cancellation of a licence or permit, and confiscation of goods and proceeds derived from criminal activity. Confiscation of property and proceeds also applies to natural persons.

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

Violation of AML Law Articles 4(2) (tipping off information regarding an investigation), 7 (failure to provide information, documents and records to MASAK or the inspectors) and 8 (record keeping) will subject the obliged party to imprisonment from one to three years.

Violation of the customer identification requirement by failing to disclose the identity of the beneficiary of a transaction will subject the perpetrator to imprisonment from six months to one year and a judicial fine up to 5,000 days.

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?

Administrative fines are assessed based on the wrongfulness of a misdemeanour, attribution of fault and economic status of the perpetrator. (Article 17 of the Misdemeanours Law (Law No. 5326).) Administrative fines are payable to the Treasury. Administrative fines are increased by the rates announced as per the Tax Procedure Law (Law No. 213) at the beginning of each calendar year. Upfront payments shall be subject to a deduction of 1/4. Collection procedures set forth under the Law on Collection Procedures for Public Receivables (Law No. 6183) shall apply. Orders (*karar*) involving administrative fines up to TL 2,000 shall be final. Orders involving administrative fines can be challenged before criminal courts of peace (*sulh ceza mahkemesi*) within 15 days of service of the notice. An upper level review is possible against the decision of the criminal courts of peace before the high criminal court (*agir ceza mahkemesi*). The decision of such court shall be final.

Judicial fines are calculated by multiplying the total number of days and the daily fine assessed in the judgment (*hüküm*) of the criminal court. Article 52 of TCL sets minimum and maximum amounts of daily judicial fine to TL 20 and TL 100, respectively. Collection procedures set forth under the Law on Collection Procedures for Public Receivables (Law No. 6183) shall apply. Public prosecutors have the authority to enforce jail terms for the unpaid term of a judicial fine. Decisions involving judicial fines or imprisonment are subject to appeal within seven days from service of notice. Appeals against judgments rendered by criminal courts of first instance are reviewed by the Regional Courts of Justice (*Bölge Adliye Mahkemesi*). Decisions of the Regional Court of Justice other than overturning a conviction can be challenged before the Court of Cassation Criminal Chamber (*Yargıtay Ceza Dairesi*) within 15 days from service of notice. Filing an appeal suspends enforcement. Appeal involves review of lawfulness of the criminal court's ruling.

The Court of Cassation may affirm, reverse, remand or modify the ruling. Regional Courts of Justice may challenge the decision of the Criminal Chamber and request that the appellate decision be reviewed by the General Assembly of Criminal Chambers (*Yargitay Ceza Genel Kurulu*). Such decision will be final.

Decisions of criminal courts of first instance and Regional Courts of Justice are not public; however, Court of Cassation decisions are published in the journal of the Court of Cassation and are available in the online database of the Ministry of Justice ("UYAP").

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 ROM, AML requirements apply to the following obliged persons (*Yukumluler*) and to their domestic and foreign (to the extent permitted by the laws of the foreign jurisdiction) agents, branches, commercial representatives and similar affiliated units:

- Banks.
- Bank card issuing organisations.
- Money lending, factoring and bureaux de change operating under the exchange legislation.
- Capital markets intermediary institutions and portfolio management companies.
- Payment institutions and electronic wire transfer institutions.
- Investment partnerships.
- Insurance, reinsurance and pension companies.
- Financial leasing companies.
- Istanbul Stock Exchange, Settlement and Custody Bank.
- Asset management companies.
- Precious metals exchange intermediaries and dealers.
- Postal service company and cargo companies.
- Real estate agents.
- Persons operating in the fields of gaming and betting including the National Lottery Administration General Directorate, Turkish Jockey Club and Spor Toto Association.
- Sports Clubs.
- Dealers selling ships, aircrafts and equipment and machinery.
- Collectors, dealers, auctioneers of art works and antiques.

In addition, the following professional services are subject to money laundering requirements as obliged persons:

- Notaries.
- Independent audit institutions licensed to audit the financial sector.
- Independent accountants (*serbest muhasebeci*), certified public accountants (*serbest muhasebeci mali müşavir*) and sworn fiscal advisors (*yeminli mali müsavir*).
- Attorneys providing consulting on the purchase and sale of real estate and formation, management and transfer of companies, foundations and associations.

Where an obliged person which has its principal place of business outside of Turkey has its agent, branch, commercial representative or a similar affiliated unit located in Turkey, the local unit will be considered an obliged person.

According to Section Two of the AML Law, obliged persons have the following AML obligations:

- *Customer identification*: Obliged parties shall identify the persons carrying out transactions and the persons on behalf or on account of whom the transactions are conducted within or through obliged parties before the transaction is completed.
- *Suspicious transaction reporting*: In case there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out, within or through the obliged parties, is acquired through illegal ways or used through illegal purposes, these transactions shall be reported to the Presidency (of MASAK) by obliged parties.
- *Implementing training, internal control and risk management systems*.
- *Periodical reporting*: Obliged persons shall report any transactions to which they are party or intermediaries that exceed the threshold amount determined by the Ministry.
- *Providing information and documents*: When requested by the Presidency or examiners, public institutions or organisations, natural and legal persons and unincorporated organisations shall provide all kinds of information, documents and related records in every type of environment, all information and passwords necessary for fully and accurately accessing to or retrieving these records and render necessary convenience.
- *Retaining and submitting of records*: The obliged parties shall retain documents, books and records, identification documents kept in every kind of environment regarding their transactions and obligations established in this Law for eight years starting from the drawn-up date, the last record date, the last transaction date, respectively, and submit them when requested.

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

Pursuant to Article 4 of ROC, only banks (excluding Central Bank of the Republic of Turkey and development and investment banks), capital markets intermediary institutions, insurance and pension companies and General Directorate of Postal Services (exclusive to banking operations) are required to maintain compliance programmes. The AML compliance programmes shall also govern the agents, branches, commercial representatives or similar affiliated units located abroad to the extent permitted by the laws of the host jurisdiction.

The AML Law requires that compliance programmes be built on a risk-based approach. Compliance programmes will contain the following measures:

- Establishing institutional policy and procedures.
- Operating risk management, monitoring and control systems.
- Establishing a compliance unit and designating a compliance officer.
- Implementing training programmes.
- Implementing internal audit systems.

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

According to Article 46 of the AML Law, obliged parties shall retain documents, books and records, identification documents kept in every kind of environment regarding their transactions and

obligations established in this Law for eight years starting from the drawn-up date, the last record date, the last transaction date, respectively, and submit them when requested. Documents and records including any supporting evidence related to suspicious transaction reporting or internal reports to compliance officers will be retained in accordance with this obligation.

ROM requires that obliged persons pay special attention to complex and unusually large transactions, which have no apparent economic or lawful purpose. Article 27 of ROM provides that suspicious transactions must be reported regardless of value. Reports must be submitted within 10 days of the date of transaction. MASAK STR Guidelines provide examples of suspicious transactions for the financial sector and other obliged persons which specify high value transactions without mentioning a threshold.

3.4 Are there any requirements to report routine 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.

Article 6 of the AML Law requires periodical reporting by obliged parties of transactions to which they are a party or acted as intermediary exceeding the threshold determined by the Ministry of Finance to the Presidency of MASAK. The Article further states that periodical reporting may also be requested from the public institutions and organisations and transaction types subject to periodic reporting, reporting procedures and periods and excluded persons will be determined by the Ministry of Finance. Secondary legislation to implement this section of the AML Law has not yet been issued.

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

According to Articles 3(c) and 4(e) of the Decree Law No. 32 regarding Protection of Value of the Turkish Currency, banks are obliged to inform the Central Bank of the Republic of Turkey of transfers abroad exceeding USD 50,000 or its equivalent in Turkish Lira or in other foreign currency. Reporting obligation excludes payments for invisible transactions involving import and export, insurance, logistics, capital movements, travel and tourism, litigation and disputes, intellectual property rights and non-profit organisations. The reporting period is 30 days from the date of transfer. Information related to large cross-border transfers is shared with Ministry of Finance, Revenue Administration and MASAK.

3.6 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 5 of ROM requires verification of customer identification (CDD):

- when a continuous business relation is established;
- when a single (or linked) transaction with an amount equal to or above TL 20,000 is carried out;
- when a single (or linked) wire transfer with an amount equal to or above TL 2,000 TL is carried out;
- in case of an STR, regardless of the amount of transaction; and
- in case of suspicion as to the accuracy and completeness of acquired identification information, regardless of the amount of transaction.

ROM requires CDD be completed prior to forming a business relationship or carrying out a transaction. Article 22 of ROM prohibits obliged persons from establishing a continuous business relationship or conducting the requested transaction, if verification of identification cannot be completed or sufficient information on the purpose of the business relationship cannot be obtained.

Articles 6 through to 12 of ROM describe types of customers and criteria for identification:

- natural persons (both Turkish and non-Turkish citizens) (Article 6);
- legal entities registered with Trade Registry (Article 7);
- associations and foundations (Article 8);
- unions and confederations (Article 9);
- political parties (Article 10);
- non-resident legal entities (Article 11); and
- unincorporated organisations (Article 12).

Verification of customer identification (including identification of persons who act on behalf of another natural person) requires presentation of identification documents such as an identification card, passport, residence permit, tax identification number, Turkish Republic identification number, bylaws and incorporation documents, trade registry documents, etc.

Legal entities: Article 7 of ROM requires verification of identity of persons authorised to represent a legal entity through registration documents of the legal entity and according to provisions of Article 6. Similar provisions are included in Articles 8-10 for associations, foundations, political parties and unincorporated organisations, except for non-resident legal entities.

Public and quasi-public institutions: Article 13 of ROM requires verification of persons acting on behalf of public and quasi-public institutions through their incumbent certificates. Identification of the customer itself can be verified through the duly issued incumbent certificate by such institutions.

Beneficial owners: Article 17/A of ROM requires verification of identification of beneficial owners. Article 3(1)(h) defines beneficial owner as "natural person(s) who ultimately control(s) or own(s); natural person acting on behalf of an obliged party, or the natural persons, legal entities or unincorporated organisations on whose behalf a transaction is carried out". Obliged parties are required to verify identification of beneficial owners holding more than 25% of shares of legal entities according to criteria set out in Article 6. Where there is suspicion that a natural person or shareholder may not be the ultimate beneficiary, or the 25% threshold is too high to verify identification of the beneficial owner, senior executives of a legal entity with ultimate representation power shall be considered as the beneficial owner. Identity of executive officers of legal entities shall be verified through commercial registry records. The same verification criteria apply to legal entity business partners in the context of establishing continuous business relations.

Simplified customer due diligence: Article 26 of ROM allows for simplified due diligence requirements, i.e. waiving the verification of identification requirement during the CDD process, where financial institutions carry out transactions among themselves, the customer is a public or quasi-public institution, a public or listed entity or the transaction involves employee pension plans. Transactions involving a foreign resident financial institution may qualify for simplified due diligence provided that the foreign institution is located in a jurisdiction that applies international AML standards and evaluation requirements.

MASAK Communiqué No. 5 expands the scope of simplified CDD to cover precious metals intermediary institutions, IMF, World Bank, development and investment banks and local consular or diplomatic units. Article 2.2.10 of the Communiqué No. 5 provides that customer identification information obtained by obliged persons operating via the internet, without forming face to face customer relationships (e.g. e-commerce companies or internet-based gaming and betting operators excluding their dealers) does not need to be verified if the customer is a Turkish resident bank and all payments will be made online or the customer is a subscriber or member who will make all payments through a bank account with matching customer identification as provided during membership application.

Obliged persons shall, on a case by case basis, assess whether a transaction presents any risk of violating the AML Laws and whether simplified CDD could apply. Obliged persons are prohibited from applying simplified CDD where there is suspicion that a money laundering offence has been committed and they are required to report such incident to Presidency of MASAK.

Enhanced customer due diligence: Article 26/A of ROM requires financial institutions to apply enhanced CDD measures for complex and high value transactions with no apparent legal or economic purpose, transactions over electronic money transfer systems and transactions and business relations with customers involving natural and legal persons resident in high risk countries. Financial institutions are required to apply additional CDD measures, such as acquiring additional information related to the customer, beneficial owner, nature and purpose of the transaction, origin of the assets and funds belonging to the customer and obtaining higher level approval for establishing a business relationship or conducting the transaction.

3.7 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?

Article 23 of ROM prohibits financial institutions from establishing correspondence relations with foreign shell banks or respondent institutions that allow shell banks to use their accounts.

Article 3(1)(f) of ROM defines financial institutions. Accordingly, the term refers to the following list:

- Banks.
- Bank card issuing organisations.
- Money lending, factoring and bureaux de change operating under the exchange legislation.
- Capital markets intermediary institutions and portfolio management companies.
- Money transfer and electronic wire transfer institutions.
- Investment partnerships.
- Insurance, reinsurance and pension companies.
- Financial leasing companies.
- Istanbul Stock Exchange, Settlement and Custody Bank.
- Postal and Telegram Association (limited to banking operations).

3.8 What is the criteria for reporting suspicious activity?

Article 4 of MASAK Communiqué No. 13 requires obliged persons to report suspicious activity, realised or attempted, where there is any document or reasonable grounds evidencing suspicion that the asset subject to the transaction relates to a money laundering offence. MASAK STR Guidelines provide criteria for the reporting requirement. Accordingly, obliged persons shall include information relating to customer profile and transaction type. Customer profile information will be based on customer identification requirements applicable to natural and legal persons including beneficiaries, their risk assessment and irregular capital, partnership and management structures.

Information related to the suspicious transaction will be based on the examples of suspicious transactions and typology of predicate offences listed in the MASAK STR Guidelines. Examination must focus on customer identification, field of activity, operation volume, nature of activity, its relation to the ordinary field of activity of the customer and the beneficiaries. Where cross-border transactions are involved, specific attention must be paid to the nature of the transaction and as to whether it fits within the ordinary field of activity of the customer. STR Guidelines list the typology of the predicate offences to provide indicators as to related categories of suspicion.

3.9 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?

Turkey has a central commercial registration system for companies, which maintains corporate information such as articles of incorporation, directors and management, corporate decisions related to capital matters and share transfers (except for bearer shares of privately held companies) and authorised representatives. Companies are registered with local units of trade registries located in the city of their head office. Any changes made to the registered information with the Trade Registry shall also be registered and announced to the public in the Turkish Trade Register Gazette. Turkish Trade Registry Gazette issues are available online at www.ticaretsicil.gov.tr in the original Turkish language. Where ultimate parent (natural or legal person) is concerned, changes to beneficial ownership taking place abroad may not be traced through the records kept with Trade Registry.

3.10 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?

Article 24 of ROM requires that customer identification information on the originator be specified in domestic or international payment orders via wire transfers of TL 2,000 or more. Financial institutions may request completion of missing identification information or return the wire transfer. Provision governs all financial institutions as defined under Article 3(1)(f) of ROM. (See also the response to question 3.7 above.)

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

Yes. For publicly traded and listed companies, bearer shares are registered with the Central Registration Agency (*Merkezi Kayıt Kurulusu*) and changes to ownership can be traced. For privately held companies, it is not mandatory to record ownership of the bearer shares in the corporate books, such as the share ledger and

transfer of such shares is not subject to the approval by the board of directors. This makes it impossible to trace changes in ownership of privately held companies with issued bearer shares.

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

Article 16 of the AML Law requires passengers who carry Turkish currency, foreign currency or instruments ensuring payment to or from abroad to disclose them fully and accurately upon request of the Customs Administration. False or misleading disclosures may subject the passenger to an administrative fine and result in the detention of the valuables by Customs Authorities. (See also the response to question 3.5 above.)

3.13 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 4 of ROM lists obliged persons subject to AML requirements in an exhaustive way. Council of Ministers has the power to expand the list of obliged persons by designating additional fields of activity for compliance with AML requirements. Obliged persons having their head office in Turkey or abroad, may apply to obtain a licence to operate in the free zones designated by the Council of Ministers, subject to the conditions set forth in the Law on Free Trade Zones (Law No. 3218) and its secondary legislation. Certain business sectors such as banks, precious metals logistics and Borsa Istanbul AS safekeeping service providers have established presence either in the form of branches or companies in the free trade zones of Turkey and their customers would also be subject to AML requirements.

4 General

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

There are no draft proposals pending at this time.

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?

Fifteenth Follow-up Report on Third Mutual Evaluation Report of FATF (2007) dated October 2014 highlighted the following areas for improvement:

- Recommendation 6 (*PEPs – politically exposed persons)*: Reviewers report that no statutory or regulatory measures have been implemented concerning establishment of customer relationships with PEPs. Turkish authorities advised that the obligation to pay special attention to risky countries would cover this measure.
- Recommendation 21 (*High-risk countries*): Article 25 of ROM requires enhanced CDD measures for natural and legal persons from risky countries. Reviewers report that the Ministry of Finance had not determined risky countries. However, Article 3(1)(i) of ROM defining "risky countries" is interpreted incorrectly by the Reviewers. The Ministry of Finance is not responsible for determining such countries. Article 3(1)(i) reads: "Risky countries are defined as those announced by the Ministry of Finance out of those which do not have sufficient AML/CFT laws and regulations, which do not cooperate or have been declared as "risky countries" by international organisations."
- Recommendation 22 (*Internal controls and foreign branches and subsidiaries*): Article 4.2 of ROM requires overseas branches, agents and commercial representatives of Turkish resident obliged persons to comply with Turkish AML requirements to the extent permitted by the host jurisdiction. Reviewers noted that there is no requirement to apply the highest of standards and no duty imposed upon the overseas branch to inform supervisors that it is unable to observe appropriate AML measures due to host country restrictions.
- Recommendation 24 (*Regulation and supervision of DNFBPs-Designated Non-Financial Businesses and Professions*): MASAK is ultimately responsible for supervising obliged parties for compliance with AML requirements. MASAK delegates this duty to examiners listed in Article 3(1)(d) of ROM. Reviewers noted that it is not clear from the list of examiners which one is responsible for supervision of each category of DNFBPs.
- Special Recommendation VII (*Wire transfers*): Tracing cross-border and domestic wire transfers, including serial payments and cover payments, is possible by including full originator and beneficiary information in a wire transfer. The AML requirement should extend over ordering, intermediary and beneficiary financial institutions and money and value transfer operators. Reviewers noted that Article 24 of ROM provides basic and limited obligation that wire transfers should only contain originator information. No information is required for intermediaries or beneficial financial institutions. In addition, it is noted that there is no provision addressing technical limitations and the issue that administrative fines applicable to violations of this requirement remain too low.

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

Turkey is not a member of the Council of Europe and therefore is not evaluated by Moneyval.

Turkey is a member of FATF and most recent FATF mutual evaluation report was published in February 2007. The most recent follow-up report on FATF MER 2007 was published in October 2014.

The IMF conducts financial system stability assessments for member countries every five years and publishes its findings and recommendations in the form of country assessment reports. The most recent IMF country assessment report for the Turkish financial sector was published in February 2017, which very broadly mentions about FATF Recommendation 6 – enhanced CDD on PEPs and including in CDD framework indicators of risky business relationships for banks – as the only areas for improvement. IMF Reviewers also recommended that BRSA's self-regulatory organisation role be elevated to a parallel FIU role along with MASAK related to suspicious transaction reporting requirements for banks and incidents of banking fraud. (See also the response to question 4.2 above.)

In our view, AML compliance is weak, and supervision is insufficient due to scarcity of law enforcement resources and lacking specialised knowledge and skills of the existing law enforcement staff. Supervision is especially deficient over unregistered foreign exchange houses, unauthorised trading companies acting as money transmitters, the unaudited non-profit sector (i.e. domestic and overseas foundations) and unauthorised gaming and betting. Deficiencies can be overcome by specialised training programmes targeting supervisors and law enforcement staff and by establishing cross-border cooperation with overseas regulators and law enforcement units.

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?

AML legislation is available online on MASAK website at www.masak.gov.tr. The materials are available in Turkish. Unofficial translations of the AML Law (Law No. 5549) and MASAK Communiqué are appended to the FATF Follow-up Report of October 2014 as Annex 4.

Prof. Av. Esra Bicen
EB LEGAL
Nisbetiye On Residence 44
Nisbetiye Cad. No. 10, Levent
Istanbul
Turkey

Tel: +90 212 283 0053
Email: ebicen@eblegal.net
URL: www.eblegal.net

Professor Bicen has 20 years of experience as a litigation and transaction lawyer in Turkey and in the United States. Her practice, lectures and publications focus on corporate, commercial (gaming, fintech, healthcare) and financial compliance, ISDA, EPC, procurement contracts and international arbitration. From 1997 to 2000, she practised with a leading Istanbul law firm specialising in international investments, cross-border financings, public tenders and dispute resolution. From 2003 to 2007, she practised complex litigation with a leading American law firm. Between 2008 and 2011, she served as a General Counsel responsible for Ernst Young Central and Southeast Europe area and headed EY's consulting firm in Turkey.

In 2011, she was appointed as a part-time faculty member at John F. Kennedy University Law School and continued her law practice with a tier-one Istanbul law firm. Since 2015, she left to dedicate her time to teaching and maintains her law practice EB LEGAL in Istanbul and Silicon Valley.

EB LEGAL | Avukatlık Bürosu
Attorneys at Law

EB LEGAL is a premier Turkish law firm offering over two decades of legal experience in Turkey and in the United States. Its combined legal expertise encompasses both civil and common law trial litigation and transaction work. This versatile legal background sets EB LEGAL apart as the epitome of a Turkish premier law firm with an evenly distributed portfolio of transactional and international arbitration clients.

EB LEGAL has the unique ability to offer full partner hands-on assistance in all assignments taken on by the firm. The firm's approach is to select the matters taken by focusing on the level of experience and sophistication required on a case-by-case basis.

EB LEGAL is a full-service firm. A representative list of industry areas served includes financial services, insurance, energy, utilities, telecommunications, media, education, automotive, pharmaceuticals, hospitals, real estate, restaurants, food and beverage, hospitality and leisure, gaming and entertainment.

United Arab Emirates

Hamdan AlShamsi

Hamdan AlShamsi Lawyers & Legal Consultants

Omar Kamel

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 the national level?

No, they are not.

2.5 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? 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 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 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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.

3.7 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 on 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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, Counsel 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 combating 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.

Omar Kamel
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: OAlSwadeh@alshamsilegal.com
URL: www.alshamsilegal.com

Omar holds a Master's Degree in Commercial law and has been a member of the Jordanian Bar since 2001. He is experienced corporate counsel and possesses strong post qualification experience in the commercial practices in MEA. He is profoundly skilled in corporate and restructuring matters, investments, corporate actions, intragroup transactions and service arrangements. Omar specialises in general mergers and acquisitions practice, strategic transactions and corporate restructurings, draft documents incidental to formation and ongoing business operations of corporations, partnerships, and limited liability companies. He also gives advice on corporate governance matters (including resolutions, preparing board and committee meeting materials and agendas and maintaining corporate records) and has experience in cross-border transactions, real estate and commercial finance transactions covering licensure, development and supply agreements.

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.

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.

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 record keeping 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 the 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.

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. However, the FCA had a number of open investigations into money laundering as at the publication of its last annual report. Anti-money laundering (**AML**) is also one of the FCA's key target areas in its current business plan. They describe their current enforcement strategy as "*where firms have poor AML controls, we will use our enforcement powers to impose business restrictions to limit the level of risk, provide deterrence messages to industry, or both. We will generally use our civil powers, but if failings are particularly serious or repeated we may use our criminal power to prosecute firms or individuals*".

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 January 2017, the FCA fined a bank GBP 163 million for failing to maintain an adequate AML framework between 2012 and 2015.

(b) 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 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 GBP3,337 in costs for laundering of around GBP100,000 in proceeds from a wine investment scam.

2.4 Are there requirements only at the 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? 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, record keeping, 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 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.

3.3 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.

3.4 Are there any requirements to report routine 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.

3.5 Are there cross-border transaction 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.

3.6 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.

3.7 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 define 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.

3.8 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).

3.9 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.

In January 2018, the UK government confirmed its intention to introduce a draft Bill before the summer recess in 2018 to establish a public register of beneficial ownership for foreign companies owning property in the UK. Formal introduction of the Bill is planned for summer 2019, with the register expected to become operational by early 2021.

3.10 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.

3.11 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.

3.12 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 3.10 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.

3.13 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?

The Sanctions and Anti-Money Laundering Bill 2017 will create a new UK legislative framework with broad powers to implement sanctions, anti-money laundering and anti-terrorist financing measures after the UK leaves the European Union.

The fifth AML Directive was agreed in December 2017 and will take effect in stages from 2019, subject to the terms of Brexit. It will expand the requirement to perform anti-money laundering checks to new categories of businesses and increase transparency requirements for the beneficial ownership of both companies and trusts.

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 FAFT report on Anti-Money Laundering and Combating the Financing of Terrorism, 16 October 2009, concluded that the UK had taken substantive action towards improving compliance with its previous core recommendation. The FAFT had found the UK partly compliant with the requirement to identify and verify beneficial owners before and during the course of establishing a business relationship. This was deemed to have been addressed by the customer due diligence framework contained in the Money Laundering Regulations 2007. As a result, the FAFT decided to remove the UK from the regular follow-up process.

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

The Fourth Round Mutual Evaluation of the UK by the FAFT is scheduled for 2018. Previous FAFT reports were conducted in October 2009 and June 2007. 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).

Acknowledgment

With thanks to the following Allen & Overy contributors for their input: Alison Cranney; Juliet de Pencier; Sarah Hitchins; Lucy Judge; Calum Macdonald; David Odejayi; Alexandra Pedder; Ian Rodgers; and Damian Ryan.

Mona Vaswani
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 20 3088 3751
Email: mona.vaswani@allenovery.com
URL: www.allenovery.com

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
One Bishops Square
London, E1 6AD
United Kingdom

Tel: +44 20 3088 2243
Email: amy.edwards@allenovery.com
URL: www.allenovery.com

Amy 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 33

USA

Stephanie Brooker

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 specified unlawful activity.

Under Section 1957, it is a crime knowingly to 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 Part 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 the 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 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. No banks or regulated financial institutions have been convicted of money laundering. Where there have been criminal cases against financial institutions, they have been under the BSA.

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, 30 regulated financial institutions (23 banks) have pled guilty or have reached criminal settlements with the Department of Justice, generally 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). There were two other BSA prosecutions of banks in the late 1980s relating to currency transaction reporting. A few settlements with foreign-owned banks have been based on alleged sanctions violations in addition to BSA violations.

In connection with some of the criminal dispositions, civil (administrative) sanctions based on the same or related misconduct have been imposed at the same time by federal 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 30 settlements under the BSA 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 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).

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 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. In addition, the Secretary of the Treasury has the legal authority to impose BSA requirements under the BSA statute, 31 U.S.C. § 5312(a)(2), on some financial and other businesses listed in the statute where FinCEN has not as yet imposed any requirements by regulation.

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 3.12.

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 and 3.2.

Currency Transaction Reporting: "Financial institutions" as defined under the BSA regulations must file Currency Transaction Reports ("CTRs"). *See* question 3.3.

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 3.3 and 3.12.

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 3.8.

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 AML Programs. *See* question 3.6.

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 3.6.

Customer Due Diligence Programs: Effective May 11, 2018, this requirement will be applicable to banks, broker-dealers, FCMs, IB-Cs, and mutual funds. *See* question 3.6.

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 or more (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 3.10.

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 virture of other business activities) are excepted from registration. 31 C.F.R. § 1022.380.

Goverment 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 discused 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 the 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, 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). Recently, in connection with an 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 controversial and 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 is due 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? 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, 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.

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 last updated in 2014. The next update is expected in 2018.

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 not 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.

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 Programs 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 currently are subject to certain requirements.

3.2 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, due diligence programs under Section 312 must be part of their AML Programs, and after May 11, 2018, the new CDD Program requirements will be part of the AML Program requirements.

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).

3.3 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.

3.4 Are there any requirements to report routine 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 3.13.

3.5 Are there cross-border transaction 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).

3.6 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 Identification Program:

As part of their AML Programs, certain financial institutions (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).

Customer Due Diligence on Non-US Private Banking Clients and Foreign Correspondents: Under the BSA, as part of their AML Programs, covered financial institutions (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 a 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).

Customer Due Diligence: To date, the only specific due diligence legal and regulatory requirements that have been implemented are the CIP requirements and the requirement to maintain due diligence programs for non-U.S. persons' private banking accounts and foreign correspondent accounts. Nevertheless, for many years, FinCEN and the federal functional regulators have 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").

In addition, as noted, pursuant to new regulatory requirements, effective May 11, 2018, as part of their AML Program, 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 CIP, obtaining information about the nature and purpose of a customer's account, ongoing monitoring of customer accounts, obtaining beneficial ownership information, and identifying a control person for legal entity customers (with certain exceptions). 31 C.F.R. § 1010.230 (beneficial ownership requirements).

3.7 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 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. Foreign correspondent banks must certify (and recertify every three years) that they are not shell banks. 31 C.F.R. § 1010.360.

3.8 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.

3.9 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.

3.10 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).

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

No, ownership of legal entities in the form of bearer shares is not permitted in the USA.

3.12 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.

3.13 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, currently, under certain circumstances, there is a requirement in seven metropolitan areas for title insurance companies to report cash sales (non-financed) of real estate at given threshold amounts depending on the area.

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.

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, Counsel 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.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Ella Alves Capone in the preparation of this chapter.

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 the White Collar Defense and Investigations Practice Group. As a prosecutor, Ms. Brooker served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia, tried 32 criminal trials, and briefed and argued criminal appeals. Ms. Brooker's practice focuses on internal investigations, regulatory enforcement, white-collar criminal defence, and compliance counseling. She represents financial institutions, multi-national companies, and individuals in connection with criminal, regulatory, and civil enforcement actions involving anti-money laundering (AML)/ Bank Secrecy Act ("BSA"), sanctions, anti-corruption, securities, tax, and wire fraud.

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.

Other titles in the ICLG series include:

- Alternative Investment Funds
- 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
- 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