International
Comparative
Legal Guides

# Anti-Money Laundering 2020

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

**Third Edition**

**Featuring contributions from:**

Allen & Gledhill LLP
Allen & Gledhill (Myanmar) Co., Ltd.
Anagnostopoulos
Ballard Spahr LLP
Beccar Varela
Blake, Cassels & Graydon LLP
CHR Legal
City Legal
Cohen & Gresser (UK) LLP
Delecroix-Gublin
DQ Advocates Limited
Enache Pirtea & Associates
Galicia Abogados, S.C.
Gibson, Dunn & Crutcher LLP
Herbert Smith Freehills LLP
JahaeRaymakers
Joyce Roysen Advogados
Kellerhals Carrard
King & Wood Mallesons
Linklaters LLP
Marxer & Partner Attorneys at Law
Morais Leitão, Galvão Teles, Soares da Silva & Associados
Nakasaki Law Firm
Nyman Gibson Miralis
Rahmat Lim & Partners
SMM Legal Maciak Mataczyński
Soemadipradja & Taher

ICLG.com

ISBN 978-1-83918-043-9
ISSN 2515-4192

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Group Publisher
Rory Smith

Publisher
Jon Martin

Editor
Amy Norton

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

# International Comparative Legal Guides

## Anti-Money Laundering 2020

### Third Edition

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

# Expert Chapters



# Q&A Chapters

# Preface

We hope that you will find this third edition of *International Comparative Legal Guide – Anti-Money Laundering* useful and informative.

This has been an active year in anti-money laundering ("AML") enforcement and compliance. There have been a number of high-profile money laundering prosecutions, investigations, and administrative enforcement actions. We have seen the implementation of the EU Fifth Anti-Money Laundering Directive. Groups such as the FATF, Wolfsberg, and the Basel Committee have been active in studying issues and updating guidance. Around the world, governments are grappling with how to apply AML controls to the digital currency industry. Nevertheless, the money laundering problem persists and sustains a wide range of criminal activity from drug trafficking, terrorism, fraud, and human trafficking, to nuclear proliferation.

In the United States, the focus has been on modernization, including how to apply the technologies of today, such as artificial intelligence and machine learning, to AML compliance. There is an ongoing assessment by the government, financial industry, and Congress on how to make the U.S. AML regime more efficient and effective and how better to promote the public and private exchange of information. Legislation is pending in Congress that may result, after years of attempts, in the establishment of a national corporate registry with beneficial ownership information for corporations and limited liability companies. Congress and financial institutions continue to seek a solution to address the inconsistency between state and federal laws on marijuana.

AML controls must be continually re-evaluated to address evolving risk. Failure to implement effective measures can have serious legal and reputational consequences for financial institutions and other businesses and their employees and immeasurable costs for the safety and well-being of society.

Gibson, Dunn & Crutcher LLP is honored to join a group of distinguished colleagues to present several articles that we hope you will find of interest on AML topics. Global Legal Group also has included chapters written by select law firms in 26 countries discussing the local AML legal and regulatory/administrative requirements and enforcement requirements. Gibson Dunn is pleased to present the chapter on the U.S. AML regime.

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

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

ICLG.com

# The International Reach of the U.S. Money Laundering Statutes


Stephanie L. Brooker


M. Kendall Day

Gibson, Dunn & Crutcher LLP

In the past decade, U.S. courts have reiterated that there is a presumption against statutes applying extraterritorially,[1] and explicitly narrowed the extraterritorial reach of the Foreign Corrupt Practices Act ("FCPA")[2] and the wire fraud statute.[3] But the extraterritorial reach of the U.S. money laundering statutes—18 U.S.C. §§ 1956 and 1957—remains uncabined and increasingly has been used by the U.S. Department of Justice ("DOJ") to prosecute crimes with little nexus to the United States. Understanding the breadth of the money laundering statutes is vital for financial institutions because these organizations often can become entangled in a U.S. government investigation of potential money laundering by third parties, even though the financial institution was only a conduit for the transactions.

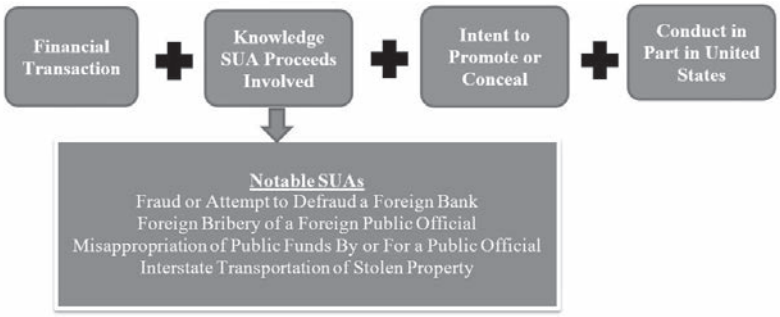
In this chapter, we examine how DOJ has stretched U.S. money laundering statutes—perhaps to a breaking point—to reach conduct that occurred outside of the United States. We begin by providing a general overview of the U.S. money laundering statutes. From there, we discuss how DOJ has relied on a broad interpretation of "financial transactions" that occur "in whole or in part in the United States" to reach, for instance, conduct that occurred entirely outside of the United States and included only a correspondent banking transaction that cleared in the United States. And while courts have largely agreed with DOJ's interpretation of the money laundering statutes, a recent acquittal by a jury in Brooklyn in a case involving money laundering charges with little nexus to the United States shows that juries occasionally may provide a check on the extraterritorial application of the money laundering statutes—for those willing to risk trial. Next, we discuss three recent, prominent examples—the FIFA corruption cases, the 1MDB fraud civil forfeitures, and the recent Petróleos de Venezuela, S.A. ("PDVSA") indictments—that demonstrate how DOJ has increasingly used the money laundering statutes in recent years to police corruption and bribery abroad. The chapter concludes by illustrating the risks that the broad reach of the money laundering statutes can have for financial institutions.

## 1 The U.S. Money Laundering Statutes and Their Extraterritorial Application

In 1980, now-Judge Rakoff wrote that "[t]o federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart—and our true love."[4] In 2020, the money laundering statutes now play as an entire string quartet for many prosecutors, particularly when conduct occurs outside of the United States.

Title 18, Sections 1956 and 1957 are the primary statutes that proscribe money laundering. "Section 1956 penalizes the knowing and intentional transportation or transfer of monetary proceeds from specified unlawful activities, while § 1957 addresses transactions involving criminally derived property exceeding $10,000 in value." *Whitfield v. United States*, 543 U.S. 209, 212-13 (2005). To prosecute a violation of Section 1956, the government must prove that: (1) a person engaged in a financial transaction; (2) knowing that the transaction involved the proceeds of some form of unlawful activity (a "Specified Unlawful Activity" or "SUA");[5] and (3) the person intended to promote an SUA or conceal the proceeds of an SUA.[6] And if the person is not located in the United States, Section 1956 provides that there is extraterritorial jurisdiction if the transaction in question exceeds $10,000 and "in the case of a non-United States citizen, the conduct occurs in part in the United States."[7] The word "conducts" is defined elsewhere in the statute as "includ[ing] initiating, concluding, or participating in initiating, or concluding a transaction."[8] Putting it all together, establishing a violation of Section 1956 by a non-U.S. citizen abroad requires:

**Figure 1: Applying Section 1956 Extraterritorially**



Section 1957 is the spending statute, involving substantially the same elements as Section 1956 but substituting a requirement that a defendant spends proceeds of criminal activity for the requirement that a defendant intends to promote or conceal an SUA.[9]

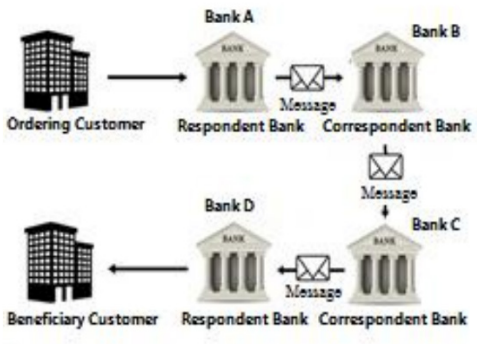
### a. "Financial Transaction" and Correspondent Banking

Although the term "financial transaction" might at first blush seem to limit the reach of money laundering liability, the reality is that federal prosecutors have repeatedly and successfully pushed the boundaries of the types of value exchanges that qualify as "financial transactions." As one commentator has noted, "virtually anything that can be done with money is a financial transaction—whether it involves a financial institution, another kind of business, or even private individuals."[10] Indeed, courts have confirmed that the reach of money laundering statutes extends beyond traditional money. One such example involves the prosecution of the creator of the dark web marketplace Silk Road. In 2013, federal authorities shut down Silk Road, which they alleged was "the most sophisticated and extensive criminal marketplace on the Internet" that permitted users to anonymously buy and sell illicit goods and services, including malicious software and drugs.[11] Silk Road's creator, Ross William Ulbricht, was charged with, among other things, conspiracy to commit money laundering under Section 1956.[12] The subsequent proceedings focused in large part on the meaning of "financial transactions" as used in Section 1956 and, specifically, whether transactions involving Bitcoin can qualify as "financial transactions" under the statute. Noting that "financial transaction" is broadly defined, the district court reasoned that because Bitcoin can be used to buy things, transactions involving Bitcoin necessarily involve the "movement of funds" and thus qualify as "financial transactions" under Section 1956.[13]

In addition to broadly interpreting "financial transaction," DOJ also has taken an expansive view of what constitutes a transaction occurring "in part in the United States"—a requirement to assert extraterritorial jurisdiction over a non-U.S. citizen.[14] One area where DOJ has repeatedly pushed the envelope involves correspondent banking transactions.

Correspondent banking transactions are used to facilitate cross-border transactions that occur between two parties using different financial institutions that lack a direct relationship. As an example, if a French company (the "Ordering Customer") maintains its accounts at a French financial institution and wants to send money to a Turkish company (the "Beneficiary Customer") that maintains its accounts at a Turkish financial institution, and if the French and Turkish banks lack a direct relationship, then often those banks will process the transaction using one or more correspondent accounts in the United States. An example of this process is depicted in Figure 2.

**Figure 2: Correspondent Banking Transactions[15]**




Although correspondent banking transactions can occur using a number of predominant currencies, such as euros, yen, and renminbi, U.S. dollar payments account for about 50 percent of correspondent banking transactions.[16] Not only that, but "[t]here are indications that correspondent banking activities in US dollars are increasingly concentrated in US banks and that non-US banks are increasingly withdrawing from providing services in this currency."[17] As a result, banks in the United States play an enormous role in correspondent banking transactions.

Given the continued centrality of the U.S. financial system, when confronted with misconduct taking place entirely outside of the United States, federal prosecutors are often able to identify downstream correspondent banking transactions in the United States involving the proceeds of that misconduct. On the basis that the correspondent banking transaction qualifies as a financial transaction occurring in part in the United States, prosecutors have used this hook to establish jurisdiction under the money laundering statutes. Two notable examples are discussed below.

#### i. *Prevezon Holdings*

The *Prevezon Holdings* case confirmed DOJ's ability to use correspondent banking transactions as a jurisdictional hook for conduct occurring overseas. The case arose from an alleged $230 million fraud scheme that a Russian criminal organization and Russian government officials perpetrated against hedge fund Hermitage Capital Management Limited.[18] In 2013, DOJ filed a civil forfeiture complaint alleging that (1) the criminal organization stole the corporate identities of certain Hermitage portfolio companies by re-registering them in the names of members of the organization. Then, (2) other members of the organization allegedly filed bogus lawsuits against the Hermitage entities based on forged and backdated documents. Later, (3) the co-conspirators purporting to represent the Hermitage portfolio companies confessed to all of the claims against them, leading the courts to award money judgments against the Hermitage entities. Finally, (4) the representatives of the purported Hermitage entities then fraudulently obtained money judgments to apply for some $230 million in fraudulent tax refunds.[19] DOJ alleged that this fraud scheme constituted several distinct crimes, all of which were SUAs supporting money laundering violations. DOJ then sought forfeiture of bank accounts and real property allegedly traceable to those money laundering violations.

The parties challenging DOJ's forfeiture action (the "claimants") moved for summary judgment on certain of the SUAs, claiming that those SUAs, including Interstate Transportation of Stolen Property ("ITSP," 18 U.S.C. § 2314), did not apply extraterritorially. The district court rejected claimants' challenge to the ITSP SUA. The court held that Section 2314 does not, by its terms, apply extraterritorially.[20] Nevertheless, the court found the case involved a permissible domestic application of the statute because it involved correspondent banking transactions. Specifically, the court held that "[t]he use of correspondent banks in foreign transactions between foreign parties constitutes domestic conduct within [the statute's] reach, especially where bank accounts are the principal means through which the relevant conduct arises."[21] In support of this holding, the court described U.S. correspondent banks as "necessary conduits" to accomplish the four U.S. dollar transactions cited by the government, which "could not have been completed without the services of these U.S. correspondent banks," even though the sender and recipient of the funds involved in each of these transactions were foreign parties.[22] The court also rejected claimants' argument that they would have had to have "purposefully availed" themselves of the services of the

correspondent banks, on the basis that this interpretation would frustrate the purpose of Section 2314 given that "aside from physically carrying currency across the U.S. border, it is hard to imagine what types of domestic conduct other than use of correspondent banks could be alleged to displace the presumption against extraterritoriality in a statute addressing the transportation of stolen property."[23]

**ii. *Boustani***

The December 2019 acquittal of a Lebanese businessman on trial in the Eastern District of New York marks an unusual setback in DOJ's otherwise successful efforts to expand its overseas jurisdiction by using the money laundering statutes and correspondent banking transactions.

Jean Boustani was an executive at the Abu Dhabi-based shipping company Privinvest Group ("Privinvest").[24] According to prosecutors, three Mozambique-owned companies borrowed over $2 billion through loans that were guaranteed by the Mozambican government.[25] Although these loans were supposed to be used for maritime projects with Privinvest, the government alleged that Boustani and his co-conspirators created the maritime projects as "fronts to raise as much money as possible to enrich themselves," ultimately diverting over $200 million from the loan funds for bribes and kickbacks to themselves, Mozambican government officials, and Credit Suisse bankers.[26] According to the indictment, Boustani himself received approximately $15 million from the proceeds of Privinvest's fraudulent scheme, paid in a series of wire transfers, many of which were paid through a correspondent bank account in New York City.[27]

Boustani did not engage directly in any activity in the United States, and he filed a motion to dismiss arguing that, with respect to a conspiracy to commit money laundering charge, as a non-U.S. citizen he must participate in "initiating" or "concluding" a transaction in the United States to come under the extraterritorial reach of 18 U.S.C. § 1956(f).[28] Specifically, he argued that "[a]ccounting interactions between foreign banks and their clearing banks in the U.S. does not constitute domestic conduct . . . as Section 1956(f) requires."[29] In response, prosecutors argued that Boustani "systematically directed $200 million of U.S. denominated bribe and kickback payments through the U.S. financial system using U.S. correspondent accounts"[30] and that such correspondent banking transactions are sufficient to allow for the extraterritorial application of Section 1956.[31]

The court agreed with the government's position. In denying the motion to dismiss, the court held that correspondent banking transactions occurring in the United States are sufficient to satisfy the jurisdictional requirements of 18 U.S.C. § 1956(f).[32] It cited to "ample factual allegations" that U.S. individuals and entities purchased interests in the loans at issue by wiring funds originating in the United States to locations outside the United States and that Boustani personally directed the payment of bribe transactions in U.S. dollars through the United States, describing this as "precisely the type of conduct Congress focused on prohibiting when enacting the money laundering provisions with which [Boustani] is charged."[33]

The jury, however, was unconvinced. After a roughly seven-week trial, Boustani was acquitted on all charges on December 2, 2019.[34] The jurors who spoke to reporters after the verdict said that a major issue for the jury was whether or not U.S. charges were properly brought against Boustani, an individual who had never set foot in the United States before his arrest.[35] The jury foreman commented, "I think as a team, we couldn't see how this was related to the Eastern District of New York."[36] Another juror echoed this sentiment, adding, "We couldn't find any evidence of a tie to the Eastern District. . . . That's why we acquitted."[37]

The *Boustani* case illustrates that even if courts are willing to accept the position that the use of correspondent banks in foreign transactions between foreign parties constitutes domestic conduct within the reach of the money laundering statute, juries may be less willing to do so.

### b. Using "Specified Unlawful Activities" to Target Conduct Abroad

Another way in which the U.S. money laundering statutes reach broadly is that the range of crimes that qualify as SUAs for purposes of Sections 1956 and 1957 is virtually without limit. Generally speaking, most federal felonies will qualify. More expansively, however, the money laundering statutes include specific foreign crimes that also qualify as SUAs. For example, bribery of a public official in violation of a foreign nation's bribery laws will qualify as an SUA.[38] Similarly, fraud on a foreign bank in violation of a foreign nation's fraud laws qualifies as an SUA.[39] In addition to taking an expansive view of what constitutes a "financial transaction" and when it occurs "in part in the United States," DOJ also has increasingly used the foreign predicates of the money laundering statute to prosecute overseas conduct involving corruption or bribery. This subsection discusses a few notable recent examples.

**i. FIFA**

In May 2015, the United States shocked the soccer world when it announced indictments of nine Fédération Internationale de Football Association ("FIFA") officials and five corporate executives in connection with a long-running investigation into bribery and corruption in the world of organized soccer.[40] Over a 24-year period, the defendants allegedly paid and solicited bribes and kickbacks relating to, among other things, media and marketing rights to soccer tournaments, the selection of a host country for the 2010 FIFA World Cup, and the 2011 FIFA presidential elections.[41] The defendants included high-level officials in FIFA and its constituent regional organizations, as well as co-conspirators involved in soccer-related marketing (*e.g.*, Traffic Sports USA), broadcasting (*e.g.*, Valente Corp.), and sponsorship (*e.g.*, International Soccer Marketing, Inc.).[42] Defendants were charged with money laundering under Section 1956(a)(2)(A) for transferring funds to promote wire fraud, an SUA.[43] Two defendants were convicted at trial.[44] The majority of the remaining defendants have pleaded guilty and agreed to forfeitures.[45]

One of the defendants, Juan Ángel Napout, challenged the extraterritorial application of the U.S. money laundering statutes. At various points during the alleged wrongdoing, Napout served as the vice president of FIFA and the president of the Confederación Sudamericana de Fútbol (FIFA's South American confederation).[46] Napout was accused of using U.S. wires and financial institutions to receive bribes for the broadcasting and commercial rights to the Copa Libertadores and Copa America Centenario tournaments.[47] He argued that the U.S. money laundering statutes do not apply extraterritorially to him and that, regardless, this exercise of extraterritorial jurisdiction was unreasonable.[48] The district court rejected these arguments, concluding that extraterritorial jurisdiction was proper because the government satisfied the two requirements in 18 U.S.C. § 1956(f): the $10,000 threshold and conduct that occurred "in part" in the United States.[49] Notably, at trial, the jury acquitted Napout of the two money laundering charges against him but convicted him on the other three charges (RICO conspiracy and two counts of wire fraud).[50] At the same trial, another defendant, José Marin, was charged with seven

counts, including two for conspiracy to commit money laundering. Marin was acquitted on one of the money laundering counts but convicted on all others.[51]

**ii. 1MDB**

The 1MDB scandal is "one of the world's greatest financial scandals."[52] Between 2009 to 2014, Jho Low, a Malaysian businessman, allegedly orchestrated a scheme to pilfer approximately $4.5 billion from 1Malaysia Development Berhad ("1MDB"), a Malaysian sovereign wealth fund created to pursue projects for the benefit of Malaysia and its people.[53] Low allegedly used that money to fund a lavish lifestyle including buying various properties in the United States and running up $85 million in gambling debts at Las Vegas casinos.[54] The former Prime Minister of Malaysia, Rajib Nazak, also personally benefited from the scandal, allegedly pocketing around $681 million.[55] Additionally, his stepson, Riza Aziz, used proceeds from the scandal to fund Red Granite Pictures, a U.S. movie production company, which produced "The Wolf of Wall Street," among other films.[56]

In 2016, DOJ filed the first of a number of civil forfeiture actions against assets linked to funds pilfered from 1MDB, totaling about $1.7 billion.[57] As the basis of the forfeiture, DOJ asserted a number of different violations of the U.S. money laundering statutes on the basis of four SUAs.[58]

In March 2018, Red Granite Pictures entered into a settlement agreement with the DOJ to resolve the allegations in the 2016 civil forfeiture action.[59] On October 30, 2019, DOJ announced the settlement of a civil forfeiture action against more than $700 million in assets held by Low in the United States, United Kingdom and Switzerland, including properties in New York, Los Angeles, and London, a luxury yacht valued at over $120 million, a private jet, and valuable artwork.[60] Although neither Red Granite Pictures nor Low challenged the extraterritoriality of the U.S. money laundering statute as applied to their property, the cases nevertheless serve as noteworthy examples of DOJ using its authority under the money laundering statutes to police political corruption abroad.

**iii. PDVSA**

To date, more than 20 people have been charged in connection with a scheme to solicit and pay bribes to officials at and embezzle money from the state-owned oil company in Venezuela, Petróleos de Venezuela, S.A.[61] The indictments charge money laundering arising from several SUAs, including bribery of a Venezuelan public official.[62]

Many of the defendants have pled guilty to the charges, but the charges against two former government officials, Nervis Villalobos and Rafael Reiter, remain pending.[63] In March 2019, Villalobos filed a motion to dismiss the FCPA and money laundering claims against him on the basis that these statutes do not provide for extraterritorial jurisdiction.[64] As to the money laundering charges, he argued that "[e]xtraterritorial jurisdiction over a non-citizen cannot be based on a coconspirator's conduct in the United States," and that extraterritorial application of the money laundering statute would violate international law and the due process clause.[65] As of this writing, the court has not ruled on the motion.

## 2 The Risks to Financial Institutions

The degree to which the U.S. money laundering statutes can reach extraterritorial conduct outside the United States has important implications for financial institutions. Prosecutions of foreign conduct under the money laundering statutes frequently involve high-profile scandals, as shown above. Financial institutions are often drawn into these newsworthy investigations. In the wake of the FIFA indictments, for instance, "[f]ederal prosecutors said they were also investigating financial institutions to see whether they were aware of aiding in the launder of bribe payments."[66] Indeed, more than half a dozen banks reportedly received inquiries from law enforcement related to the FIFA scandal.[67]

At a minimum, cooperating with these investigations is time-consuming and costly. The investigations can also create legal risk for financial institutions. In the United States, "federal law generally imposes liability on a corporation for the criminal acts of its agents taken on behalf of the corporation and within the scope of the agent's authority via the principle of *respondeat superior*, unless the offense conduct solely furthered the employee's interests at the employer's expense (for instance, where the employee was embezzling from the employer)."[68] And prosecutors can satisfy the intent required by arguing that individual employees were "deliberately ignorant" of or "willfully blind" to, for instance, clearing suspicious transactions.[69]

The wide scope of potential corporate criminal liability in the United States is often surprising to our clients, particularly those with experience overseas where the breadth of corporate liability is narrower than in the United States. As one article explained, the *respondeat superior* doctrine is "exceedingly broad" as "it imposes liability regardless of the agent's position in the organization" and "does not discriminate" in that "the multinational corporation with thousands of employees whose field-level salesman commits a criminal act is as criminally responsible as the small corporation whose president and sole stockholder engages in criminal conduct."[70]

Given the breadth of corporate criminal liability, DOJ applies a 10-factor equitable analysis to determine whether to impute individual employee liability to the corporate employer. These 10 factors are the "Principles of Federal Prosecution of Business Organizations," and are often referred to by the shorthand term "Filip Factors." The factors include considerations such as the corporation's cooperation, the pervasiveness of the wrongdoing, and other considerations meant to guide DOJ's discretion regarding whether to pursue a corporate resolution.[71] They are not equally weighted (indeed, there is no specific weighting attached to each, and the DOJ's analysis will not be mathematically precise). Financial institutions should continually assess, both proactively and in the event misconduct occurs, the actions that can be taken to ensure that they can persuasively argue that, even if there is legal liability under the doctrine of *respondeat superior*, prosecution is nevertheless unwarranted under the Filip Factors.

## 3 Conclusion

In recent years, DOJ has expansively applied the money laundering statutes to reach extraterritorial conduct occurring almost entirely overseas. Indeed, a mere correspondent banking transaction in the United States has been used by DOJ as the hook to prosecute foreign conduct under the U.S. money laundering statutes. Because of the extraordinary breadth of corporate criminal liability in the United States, combined with the reach of the money laundering statutes, the key in any inquiry is to quickly assess and address prosecutors' interests in the institution as a subject of the investigation.

## Acknowledgment

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

## Note

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

## Endnotes

1. *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010).
2. *United States v. Hoskins*, 902 F.3d 69 (2d Cir. 2018). Although the Second Circuit rejected the government's argument that Hoskins could be charged under the conspiracy and complicity statutes for conduct not otherwise reachable by the FCPA, *id.* at 97, he was nevertheless found guilty at trial in November 2019 on a different theory of liability: that he acted as the agent of Alstom S.A.'s American subsidiary. *See* Jody Godoy, *Ex-Alstom Exec Found Guilty On 11 Counts In Bribery Trial*, Law360 (Nov. 8, 2019), https://www.law360.com/articles/1218374/ex-alstom-exec-found-guilty-on-11-counts-in-bribery-trial.
3. *See, e.g.*, *United States v. Elbaz*, 332 F. Supp. 3d 960, 974 (D. Md. 2018) (collecting cases where extraterritorial conduct was not subject to the wire fraud statute).
4. Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 Duq. L. Rev. 771, 822 (1980).
5. Many of the SUAs covered by Section 1956 are incorporated by cross-references to other statutes. *See* 18 U.S.C. § 1956(c)(7). All of the predicate acts under the Racketeer Influenced and Corrupt Organizations Act, for instance, are SUAs under Section 1956. 18 U.S.C. § 1956(c)(7)(a). One commentator has estimated that there are "250 or so" predicate acts in Section 1956. Stefan D. Cassella, *The Forfeiture of Property Involved in Money Laundering Offenses*, 7 Buff. Crim. L. Rev. 583, 612 (2004). Another argues this estimate is "exceptionally conservative." Charles Doyle, Cong. Research Serv., RL33315, *Money Laundering: An Overview of 18 U.S.C. § 1956 and Related Federal Criminal Law* 1 n.2 (2017).
6. *See, e.g.*, Fifth Circuit Pattern Jury Instructions (Criminal Cases) Nos 2.76A, 2.76B, *available at* http://www.lb5.uscourts.gov/viewer/?/juryinstructions/Fifth/crim2015.pdf; Ninth Circuit Manual of Model Criminal Jury Instruction Nos 8.147–49, *available at* http://www3.ce9.uscourts.gov/jury-instructions/sites/default/files/WPD/Criminal_Instructions_2019_12_0.pdf.
7. 18 U.S.C. § 1956(f).
8. 18 U.S.C. § 1956(c)(2).
9. *See, e.g.*, Fifth Circuit Pattern Jury Instructions (Criminal Cases) No. 2.77; Ninth Circuit Manual of Model Criminal Jury Instruction No. 8.150.
10. Stefan D. Cassella, *The Money Laundering Statutes (18 U.S.C. §§ 1956 and 1957)*, The United States Attorneys' Bulletin, Vol. 55, No. 5 (Sept. 2007); *see also* 18 U.S.C. § 1956(c)(4)(i) (definition of "financial transaction").
11. *United States v. Ulbricht*, 31 F. Supp. 3d 540, 549–50 (S.D.N.Y. 2014).
12. *Id.* at 568–69.
13. *Id.* Ultimately, Ulbricht was convicted and his conviction was affirmed on appeal. *See United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017). The Second Circuit did not address the district court's interpretation of the term "financial transactions" under Section 1956.
14. 18 U.S.C. § 1956(f)(1).
15. International Monetary Fund, *Recent Trends in Correspondent Banking Relationships: Further Considerations*, at 9 (Apr. 21, 2017), https://www.imf.org/en/Publications/Policy-Papers/Issues/2017/04/21/recent-trends-in-correspondent-banking-relationships-further-considerations.
16. *Id.*
17. Bank for International Settlements Committee on Payments and Market Infrastructures, *Correspondent Banking*, at 12 (July 2016), https://www.bis.org/cpmi/publ/d147.pdf.
18. *See generally* Bill Browder, *Red Notice: A True Story of High Finance, Murder, and One Man's Fight for Justice* (2015). The alleged scheme was discovered by Russian tax lawyer Sergei Magnitsky, who was arrested on specious charges and died after receiving inadequate medical treatment in a Russian prison. In response to Magnitsky's death, the United States passed a bill named after him sanctioning Russia for human rights abuses. *See* Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012, Pub. L. 112–208 (2012).
19. Second Amended Complaint at 10–12, *United States v. Prevezon Holdings Ltd.*, No. 13-cv-06326 (S.D.N.Y. Oct. 23, 2015), ECF No. 381.
20. *United States v. Prevezon Holdings Ltd.*, 251 F. Supp. 3d 684, 691-92 (S.D.N.Y. 2017).
21. *Id.* at 692.
22. *Id.* at 693.
23. *Id.*
24. Stewart Bishop, *Boustani Acquitted in $2B Mozambique Loan Fraud Case*, Law360 (Dec. 2, 2019), https://www.law360.com/articles/1221333/boustani-acquitted-in-2b-mozambique-loan-fraud-case.
25. Superseding Indictment at 6, *United States of America v. Boustani et al.*, No. 1:18-cr-00681 (E.D.N.Y. Aug. 16, 2019), ECF No. 137.
26. *Id.* at 6–7.
27. *Id.* at 33.
28. Motion to Dismiss at 35–36, *United States of America v. Boustani et al.*, No. 1:18-cr-00681 (E.D.N.Y. June 21, 2019), ECF No. 98.
29. *Id.* at 36.
30. Opposition to Motion to Dismiss at 38, *United States of America v. Boustani et al.*, No. 1:18-cr-00681 (E.D.N.Y. July 22, 2019), ECF No. 113.
31. *Id.* at 34–35 (citing *United States v. All Assets Held at Bank Julius* ("*All Assets*"), 251 F. Supp. 3d 82, 96 (D.D.C. 2017).)
32. Decision & Order Denying Motions to Dismiss at 14, *United States of America v. Boustani et al.*, No. 1:18-cr-00681 (E.D.N.Y. Oct. 3, 2019), ECF No. 231.
33. *Id.* at 15–16; *see also All Assets*, 251 F. Supp. 3d at 95 (finding correspondent banking transactions fall within U.S. money laundering statutes because "[t]o conclude that the money laundering statute does not reach [Electronic Fund Transfers] simply because [defendant] himself did not choose a U.S. bank as the correspondent or intermediate bank for his wire transfers would frustrate Congress's intent to prevent the use of U.S. financial institutions 'as clearinghouses for criminals'"). In *United States v. Firtash*, No. 13-cr-515, 2019 WL 2568569 (N.D. Ill. June 21, 2019), the defendant recently moved to dismiss an indictment on grounds including that correspondent banking transactions do not fall within the scope of the U.S. money laundering statute. The court has sidestepped the argument for now, concluding that this argument "does not support dismissal of the Indictment at this stage" because "the Indictment does not specify that the government's proof is limited to correspondent bank transactions." *Id.* at *9.
34. Stewart Bishop, *Boustani Acquitted in $2B Mozambique Loan Fraud Case*, Law360 (Dec. 2, 2019), https://www.law360.com/articles/1221333/boustani-acquitted-in-2b-mozambique-loan-fraud-case.
35. *Id.*

36. *Id.*
37. *Id.*
38. 18 U.S.C. § 1956(c)(7)(B)(iv). In *United States v. Chi*, 936 F.3d 888, 890 (9th Cir. 2019), the Ninth Circuit recently rejected the argument that the term "bribery of a public official" in Section 1956 should be read to mean bribery under the U.S. federal bribery statute, as opposed to the article of the South Korean Criminal Code at issue in that case.
39. 18 U.S.C. § 1956(c)(7)(B)(iii).
40. U.S. Dep't of Justice, *Attorney General Loretta E. Lynch Delivers Remarks at Press Conference Announcing Charges Against Nine FIFA Officials and Five Corporate Executives* (May 27, 2015), https://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-press-conference-announcing-charges.
41. Superseding Indictment at ¶¶ 95–360, *United States v. Hawit*, No. 15-cr-252 (E.D.N.Y. Nov. 25, 2015), ECF No. 102.
42. *See, e.g.*, *id.* at ¶¶ 30–93.
43. *See, e.g.*, *id.* at ¶ 371.
44. Press Release, U.S. Dep't of Justice, High-Ranking Soccer Officials Convicted in Multi-Million Dollar Bribery Schemes (Dec. 26, 2017), https://www.justice.gov/usao-edny/pr/high-ranking-soccer-officials-convicted-multi-million-dollar-bribery-schemes.
45. U.S. Dep't of Justice, *FIFA Prosecution United States v. Napout et al.* and Related Cases, Upcoming Court Dates, https://www.justice.gov/usao-edny/file/799016/download (last updated Nov. 5, 2019).
46. Superseding Indictment, *supra* note 41, at ¶ 41.
47. Superseding Indictment, *supra* note 41, at ¶¶ 376–81, 501–04.
48. Memorandum of Law in Support of Defendant Juan Angel Napout's Motion to Dismiss All Charges for Lack of Extraterritorial Jurisdiction, at 3–4, *Hawit*, *supra* note 41, ECF No. 491-1.
49. *United States v. Hawit*, No. 15-cr-252, 2017 WL 663542, at *8 (E.D.N.Y. Feb. 17, 2017).
50. *United States v. Napout*, 332 F. Supp. 3d 533, 547 (E.D.N.Y. 2018).
51. *Id.* On appeal, Napout challenged the extraterritoriality of the honest-services wire-fraud statutes, a case currently pending before the Second Circuit. *See United States of America v. Webb et al.*, No. 18-2750 (2d. Cir. appeal docketed Sept. 17, 2018), Dkt. 107. Marin did not raise the extraterritoriality of the money laundering statute on appeal. *Id.*, Dkt. 104.
52. Heather Chen, Mayuri Mei Lin, and Kevin Ponniah, *1MDB: The Playboys, PMs and Partygoers Around a Global Financial Scandal*, BBC (Apr. 2, 2019), https://www.bbc.com/news/world-asia-46341603; *see generally* Tom Wright & Bradley Hope, *Billion Dollar Whale: The Man Who Fooled Wall Street, Hollywood, and the World* (2018).
53. Complaint at 6, *United States v. "The Wolf of Wall Street,"* No. 2:16-cv-05362 (C.D. Cal. July 20, 2016), ECF No. 1, https://www.justice.gov/archives/opa/page/file/877166/download.
54. Complaint, *supra* note 53, at 37.
55. *Najib 1MDB Trial: Malaysia Ex-PM Faces Court in Global Financial Scandal*, BBC (Apr. 3, 2019), https://www.bbc.com/news/world-asia-47194656. In the aftermath of the scandal, Nazak was voted out of office and currently faces trial in Malaysia. *Id.*
56. Complaint, *supra* note 53, at 63–65.
57. Complaint, *supra* note 53; Rishi Iyengar, *'Wolf of Wall Street' Maker Settles US Lawsuit for $60 Million*, CNN Business (Mar. 7, 2018), https://money.cnn.com/2018/03/07/media/wolf-wall-street-red-granite-1mdb-settlement/index.html.
58. *See* Complaint, *supra* note 53, at 132.
59. Consent Judgment of Forfeiture, No. 2:16-cv-05362 (C.D. Cal. Mar. 8, 2018), ECF No. 143. As a part of the settlement, Red Granite Pictures agreed to forfeit $60 million. *Id.* at 5.
60. *See United States v. Any Rights to Profits, Royalties and Distribution Proceeds Owned by or Owed Relating to EMI Music Publishing Group*, Stipulation and Request to Enter Consent Judgment of Forfeiture, No. 16-cv-05364 (C.D. Cal. Oct. 30, 2019), ECF No. 180; Press Release, U.S. Dep't of Justice, United States Reaches Settlement to Recover More Than $700 Million in Assets Allegedly Traceable to Corruption Involving Malaysian Sovereign Wealth Fund (Oct. 30, 2019), https://www.justice.gov/opa/pr/united-states-reaches-settlement-recover-more-700-million-assets-allegedly-traceable.
61. *See* Indictment, *United States v. De Leon-Perez et al.*, No. 4:17-cr-00514 (S.D. Tex. Aug. 23, 2017), ECF No. 1; Press Release, U.S. Dep't of Justice, Two Members of Billion-Dollar Venezuelan Money Laundering Scheme Arrested (July 25, 2018), https://www.justice.gov/opa/pr/two-members-billion-dollar-venezuelan-money-laundering-scheme-arrested.
62. Criminal Information at 1–2, *United States v. Krull*, No. 1:18-cr-20682 (S.D. Fla. Aug. 16, 2018), ECF No. 23; Criminal Complaint at 6, *United States v. Guruceaga, et al.*, No. 18-MJ-03119 (S.D. Fla. July 23, 2018), ECF No. 3.
63. Press Release, U.S. Dep't of Justice, Former Venezuelan Official Pleads Guilty to Money Laundering Charge in Connection with Bribery Scheme (July 16, 2018), https://www.justice.gov/opa/pr/former-venezuelan-official-pleads-guilty-money-laundering-charge-connection-bribery-scheme-0.
64. *See* Defendant's Motion to Dismiss at 9–24, *United States v. Villalobos*, No. 4:17-cr-00514 (S.D. Tex. Mar. 28, 2019), ECF No. 123.
65. *See id.* at 21–35.
66. Gina Chon & Ben McLannahan, *Banks face US investigation in Fifa corruption scandal*, *Financial Times* (May 27, 2015); *see also* Christie Smythe & Keri Geiger, *U.S. Probes Bank Links in FIFA Marketing Corruption Scandal*, Bloomberg (May 27, 2015).
67. Christopher M. Matthews & Rachel Louise Ensign, *U.S. Authorities Probe Banks' Handling of FIFA Funds*, *Wall St. Journal* (July 23, 2015).
68. *Fed. Ins. Co. v. United States*, 882 F.3d 348, 368 (2d Cir. 2018).
69. *See, e.g.*, *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011); *United States v. Florez*, 368 F.3d 1042, 1044 (8th Cir. 2004).
70. Philip A. Lacovara & David P. Nicoli, *Vicarious Criminal Liability of Organizations: RICO as an Example of a Flawed Principle in Practice*, 64 St. John's L. Rev. 725, 725–26 (1990).
71. *See* U.S. Department of Justice, *Principles of Federal Prosecution of Business Organizations* (Aug. 28, 2008), https://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

**Stephanie L. Brooker**, former Director of the Enforcement Division at the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN), the lead U.S. anti-money laundering regulator, and a former federal prosecutor, is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. She is Co-Chair of the Financial Institutions Practice Group and a member of White Collar Defense and Investigations Practice Group. As a prosecutor, Ms. Brooker tried 32 criminal trials, investigated a broad range of white-collar and other federal criminal matters, briefed and argued criminal appeals, and served as the Chief of the Asset Forfeiture and Money Laundering Section in the U.S. Attorney's Office for the District of Columbia. Ms. Brooker's practice focuses on internal investigations, regulatory enforcement defense, white-collar criminal defense, and compliance counseling. Her practice focuses on internal investigations, regulatory enforcement defense and white-collar criminal defense on a wide range of issues, including: sanctions; anti-corruption; anti-money laundering/Bank Secrecy Act; securities violations; tax and wire fraud; MeToo matters; and employment matters. She also regularly advises corporate clients, boards of directors, and trade associations on compliance policies and issues and forfeiture matters. Ms. Brooker was named a *National Law Journal* White Collar Trailblazer and a *Global Investigations Review* Top 100 Women in Investigations.

**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

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

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

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

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

# The Intersection of Money Laundering and Real Estate


Peter D. Hardy


Priya Roy


Terence M. Grugan


Mary K. Treanor

Ballard Spahr LLP

## Introduction: An Increasing Focus on Money Laundering Through Real Estate

The use of real estate to launder money is a global concern. In the U.S., regulators and prosecutors steadily have warned that money launderers located both at home and abroad target U.S. real estate transactions because they are a relatively effective and anonymous means of "cleaning" dirty money. For example, in August 2017, the Financial Crimes Enforcement Network, or FinCEN, issued an "Advisory to Financial Institutions and Real Estate Firms and Professionals"[1] which asserted that the real estate industry is vulnerable to abuse by illicit actors looking to launder criminal proceeds specifically. FinCEN attributed this vulnerability to the fact that the value of high-end properties tends to appreciate over time and can shield the owner from currency fluctuations and market instability. Further, through the purchase of luxury property, illicit actors can clean large sums of money in a single transaction.

Director of FinCEN Kenneth Blanco repeatedly has remarked that a key vulnerability of the U.S. real estate industry is the use of shell companies[2] – anonymity representing the most basic and pernicious anti-money laundering ("AML") problem across the globe. Although FinCEN's relatively new Customer Due Diligence regulation,[3] which requires the collection of beneficial ownership information for legal entities when opening an account at a bank or other financial institution, has partially addressed this vulnerability in the U.S., Director Blanco also has acknowledged that the U.S. is increasingly perceived abroad as a haven for money launderers.[4]

Likewise, in its 2020 National Strategy for Combating Terrorist and Other Illicit Financing ("2020 Treasury Report"),[5] the U.S. Department of Treasury highlighted the risk that anonymous companies or straw purchasers can use real estate transactions to purchase high-value assets that maintain relatively stable value. This risk is both domestic and foreign and is especially significant for all-cash purchases, which do not require information on the source of funds or identification of a beneficial owner. According to 2020 Treasury Report, "anonymity in real estate purchases can be abused in the same way as anonymity in financial services" and a legislative solution is needed.

Concern by U.S. regulators about real estate has not occurred in a vacuum. The Financial Action Task Force ("FATF"), an international AML watchdog group, issued a 2016 report finding that U.S. regulators' failure to address and regulate real estate transactions caused it to lag behind its global partners in effective AML regulations.[6] The report highlighted the fact that U.S. real estate professionals were not required to systematically apply basic or enhanced due diligence processes to their customers, including gathering information regarding beneficial ownership information. FATF also noted that 25 per cent of the U.S. real estate market does not involve financing – particularly in high-end transactions. Although FATF acknowledged the limited role of real estate agents, it stated that they did not "appear to understand what the [money laundering] risks in relation to high-end real estate are or what the appropriate mitigation measures would be".

Despite the explicit inclusion of "persons involved in real estate closings and settlements" in the definition of a "financial institution" under the Bank Secrecy Act ("BSA"),[7] FinCEN to date has not issued regulations regarding real estate brokers, escrow agents, title insurers, and other real estate professionals.[8] Nonetheless, FinCEN has responded to the above concerns by engaging in years of *de facto* regulation as to certain businesses by issuing Geographic Targeting Orders ("GTOs"), beginning in 2016. The GTOs reflect FinCEN's increasing interest in the real estate industry, and strongly suggest that data collected through the GTOs will be used to support proposed BSA/AML law or regulation regarding the real estate industry.

As noted, concerns over money laundering and real estate are global. As an example, we will discuss the U.K., which has emerged as a perceived safe haven for money launderers looking to take advantage of a high-end real estate market, particularly in London. As in the U.S., the core problems are anonymity, the use of shell companies, and lack of beneficial ownership information.

Finally, and regardless of any AML regulatory requirements, real estate professionals – like all professionals – always are subject to the basic U.S. criminal money laundering statutes, which prohibit engaging in or aiding and abetting money laundering. The key issue in such investigations and prosecutions often is whether the professional knew that the transaction involved tainted money. Civil forfeiture of real estate properties also remains a risk for industry professionals.

## Current U.S. AML Considerations for the Real Estate Industry

### GTOs

Since 2016, FinCEN has issued GTOs which impose requirements on title insurance companies for transactions occurring in particular U.S. locations for transactions that are not financed by loans from financial institutions. Since then, FinCEN has extended the GTOs every six months.[9]

Specifically, U.S. title insurance companies must identify the natural persons behind legal entities used in purchases of residential real estate performed without a bank loan or similar form of external financing. Title insurance companies must file

a special Currency Transaction Report, or CTR. These records must be retained for five years from the last effective day of the most recent GTO and must be available to FinCEN and to law enforcement upon appropriate requests.

The GTOs currently apply only to "Covered Businesses", which are defined as title insurance companies and their subsidiaries. As of April 2020, a "Covered Transaction" is defined as:

- a cash transaction – including a currency, cashier's cheque, certified cheque, traveller's cheque, personal cheque, business cheque, money order in any form, funds transfer or virtual currency – including a transaction in which only a part of the purchase price was made using one of these methods of payments;
- without a bank loan or similar form of external financing;
- of residential real property;
- with a purchase price of $300,000 or more; and
- purchased by a "Legal Entity." A "Legal Entity" is broadly defined and includes a corporation, limited liability company, partnership or other similar business entity, formed under the laws of the U.S. or any foreign jurisdiction.

The filed report must include the following information:

- the legal entity making the purchase;
- the individual responsible for representing the legal entity, that is an individual authorised by the entity to enter legally binding contracts on behalf of the entity; and
- the beneficial owner(s) of the legal entity, among other detailed information about the parties involved in the all-cash transaction.

The "beneficial owner" who must be identified is defined as "each individual who, directly or indirectly, owns 25 per cent or more of the equity interests of the Legal Entity purchasing real property in the Covered Transaction". This definition tracks the Beneficial Ownership rule issued by FinCEN for customer due diligence for new legal entity accounts by focusing on 25 per cent or more ownership percentage, but it differs from the Beneficial Ownership rule by not including a "control" prong in its definition of a beneficial owner. FinCEN has stated that a Covered Business can rely on documents presented to it when investigating the beneficial owner of a legal entity.[10]

Under the GTO issued in November 2019, the following nine districts are included:

- California: San Diego; Los Angeles; San Francisco; San Mateo; and Santa Clara Counties.
- Florida: Miami-Dade; Broward; and Palm Beach Counties.
- Hawaii: City and County of Honolulu.
- Illinois: Cook County.
- Massachusetts: Suffolk and Middlesex Counties.
- Nevada: Clark County.
- New York: Boroughs of Brooklyn; Queens; Bronx; Staten Island; and Manhattan.
- Texas: Bexar; Tarrant; and Dallas Counties.
- Washington: King County.

The 2020 Treasury Report confirmed that the government regards the GTOs as valuable investigative leads and included statistics on the types of information that FinCEN has been able to gather from the GTOs.

- 6,303 transactions (35 per cent of all reported transactions) involved subjects identified in a Suspicious Activity Report ("SAR"), and of those transactions, 1,082 matched to higher-risk SARs.
- 2,002 transactions (11 per cent of all reported transactions) involved a foreign beneficial owner or purchaser representative.
- 385 of those foreign buyer-transactions (or 19 per cent) involved a foreign beneficial owner or purchaser representative who is the subject of a SAR.
- Foreign buyers are disproportionately likely to be the subject of a higher risk SAR – 206 of the 385 foreign buyer-transactions with a related SAR (or 54 per cent) involved SAR reporting high-risk activity: more than three times the rate for domestic buyers (15 per cent).

The 2020 Treasury Report also cites a study finding that all-cash purchases by legal entities declined by 70 per cent immediately following the first real estate GTO. The 2020 Treasury Report concludes that the study "suggests that transparency initiatives like the GTOs have an impact in markets where anonymity is highly valued, but also highlights the need for a more comprehensive and permanent solution".

As noted, FinCEN issued in August 2017 an Advisory on the real estate industry which indicated FinCEN's growing concern with money laundering risks in the industry. Although the Advisory created no legal obligations, it suggested practices that it expected industry members to be aware of. The Advisory urged real estate professionals to voluntarily file SARs to report suspicious transactions. It is clear from the Advisory that FinCEN believes that real estate professionals "are well-positioned to identify potentially illicit activity as they have access to a more complete view and understanding of the real estate transaction and of those involved in the transaction". FinCEN listed certain facts and circumstances that may lead to such a filing, such as when the transaction:

- lacks economic sense or has no apparent lawful business purpose. Suspicious real estate transactions may include purchases/sales that generate little to no revenue or are conducted with no regard to high fees or monetary penalties;
- is used to purchase real estate with no regard for the property's condition, location, assessed value, or sale price;
- involves funding that far exceeds the purchaser's wealth, comes from an unknown origin, or is from or goes to unrelated individuals or companies; or
- is deliberately conducted in an irregular manner. Illicit actors may attempt to purchase property under an unrelated individual's or company's name or ask for records (e.g., assessed value) to be altered.

The above potential red flags also may guide the filing of GTOs: the CTR form used for such filings contains a box to be checked when the transaction is also regarded as "suspicious".

## Non-Bank Residential Mortgage Lenders and Originators ("RMLOs")

The BSA defines a "financial institution" to include, among other things, a loan or finance company.[11] This term remained undefined until 2009, when FinCEN issued a proposed rule soliciting comments on whether to include RMLOs in the definition of a "loan or finance company" for the purpose of requiring them to establish AML programmes and to report suspicious activities under the BSA.[12] In 2012, FinCEN issued a final rule providing that loan or finance companies included (only) RMLOs, and requiring RMLOs to establish AML programmes and file SARs when required.[13] When issuing this rule, FinCEN noted that its requirement was motivated in part by FinCEN's finding that "independent mortgage lenders and brokers originated many of the mortgages that were the subject of bank SAR filings". FinCEN has defined a RMLO as "[a] person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage loan", but has excluded individuals financing the sale of their own property.[14] Importantly, the definition is limited to mortgage loans involving residential properties containing only one to four units.

Over 17 years ago, in April 2003, FinCEN more broadly issued an advanced notice of proposed rulemaking regarding AML programme requirements for persons involved in real estate closings and settlements[15] – but it never issued a final rule. Now, given the data from years of GTOs, coupled with the heightened global scrutiny of the real estate industry, such regulations finally may occur.

## Recent Proposals to Expand BSA/AML Duties as to Real Estate Transactions

Although the GTO programme has been successful and FinCEN repeatedly has expanded its scope since 2016, the GTOs, by their very nature, leave open wide swaths of the real estate industry and uncovered the vast majority of the country. Recently, Congress has attempted to fill those gaps through legislation intended to make GTOs permanent and to expand their reach nationwide.

Under the Defending American Security from Kremlin Aggression Act ("DASKAA"), a sanctions bill targeting Russian interests[16] introduced in the U.S. Senate on February 13, 2019, title insurance companies would have to "obtain, maintain, and report to the Secretary information on the beneficial owners of entities that purchase residential real estate in high-value transactions in which the domestic title insurance company is involved".[17] "Beneficial Owner" would retain its definition in the GTO programme, applying to all 25 per cent or more interest holders in an acquiring entity.[18] Because the requirements would apply nationwide, FinCEN would be required to establish appropriate monetary thresholds based on the real estate market at issue.[19]

Additionally, legislation entitled "Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings" (the "ILLICIT CASH Act") was introduced in June 2019.[20] This legislation calls for the expansion of the GTOs by imposing reporting obligations on "any person involved in a transaction related to the purchase and sale of real estate". The scope of this expansion continues to be uncertain, including whether it would apply to both residential and commercial transactions. On October 23, 2019 the U.S. House passed H.R. 2513,[21] a two-part Act which sets forth in its initial section the Corporate Transparency Act ("CTA"). The CTA would require defined U.S. companies to report identifying information on their beneficial owners to the Treasury Department – so that such information would be available to both the government and financial institutions performing their own AML duties.

However, it is far from certain that any of the above proposals will become law, at least in the foreseeable future. In the meantime, FinCEN continues renewing its targeted GTOs.

## AML Considerations for Real Estate in Europe: A U.K. Case Study

Concerns over money laundering and real estate are hardly confined to the U.S. We will discuss here the U.K., which has emerged as a perceived safe haven for money launderers looking to stash their ill-gotten gains in a reliable and expensive real estate market. The U.K.'s Treasury Department has identified real estate as a "weak link" in the U.K.'s AML regime.[22] Indeed, an estimated £4.4 billion ($5.7 billion) of investment in U.K. real estate stems from "politically exposed persons ["PEPs"] in high-corruption-risk jurisdictions".[23] Until recently, the U.K. lacked the laws and accompanying regulations to effectively address money laundering via real estate.

In April 2016, the explosive Panama Papers ("Papers") scandal underscored this vulnerability. It revealed that, among other things, 2,800 companies registered overseas were connected to over 6,000 title deeds in the U.K. worth at least £7 billion.[24] The Papers also shed light on a number of alleged high-profile money laundering schemes impacting the U.K., including one perpetrated by Pakistan's then-prime minister, Nawaz Sharif. Specifically, the Papers revealed Sharif's purchase – via his then-minor children – of a luxury London property through offshore companies in the British Virgin Islands in the mid-1990s. Following these revelations, Sharif was sentenced to 10 years in prison arising from charges that he used a complex series of transactions and shell companies to funnel the proceeds of public funds embezzled from Pakistan into assets in London.[25]

In a more recent example, separate from the Papers, the stepson of the Malaysian prime minster, Riza Aziz, allegedly used funds originally from 1Malaysia Development Bhd ("1MDB") – at the heart of a massive international money laundering scandal – to purchase a £23.25 million property in London.[26] These are just two examples out of the many that abound.[27]

Transparency International UK, a watchdog at the forefront of international money laundering, points to the following (among other) factors as indicative of the vulnerability of the U.K.'s real estate sector: (1) the use of anonymous and opaque corporate structures to purchase property – as was the case with Mr. Aziz; (2) PEPs owning luxury property; and (3) lax AML compliance in the private sector.[28] As a result of these vulnerabilities, the U.K. – and especially London – has become a haven for international money launderers. This, in turn, has driven up the price of U.K. real estate and made it increasingly less affordable for the average resident.[29]

In an effort to combat money laundering via real estate, the U.K. has sought to enact a variety of legislative reforms in recent years targeting this industry. Following the May 2016 Global Anti-Corruption Summit hosted in London, the U.K. announced it would be introducing a public beneficial ownership register of overseas companies that own U.K. land titles.[30] The bill – not yet passed – seeks to identify the true ownership of properties to better identify those properties purchased through illicit proceeds. The government intends to make the registry public by 2021 and owners who fail to comply with the directive could be sent to prison for two years and fined.[31]

In addition, since 2017, the U.K. has required real estate agents to comply with "know your customer" requirements on buyers and sellers. These requirements include collecting documents verifying a seller's or buyer's identity and address and typically requires agents to meet their clients face-to-face and assess whether their explanation for their wealth appears plausible.[32]

Moreover, in January 2018, the U.K. enacted an order – titled an "Unexplained Wealth Order" – that empowers certain enforcement agencies to investigate and seize assets over £50,000 owned by a person "who is reasonably suspected of involvement in, or of being connected to a person involved in, serious crime".[33] U.K. law enforcement has implemented this new tool and, later in 2018, used it to investigate how Zamira Hajiyeva, wife of an Azerbaijani banker, purchased a £11.5 million house in London based on her husband's government salary. Her husband was subsequently sentenced to 15 years in prison for fraud and embezzlement.[34]

Finally, in another show of the U.K.'s enhanced scrutiny of the real estate sector, Her Majesty's Revenue & Customs ("HMRC") in March 2019 launched its most high-profile crackdown to date on the sector, raiding 50 real estate agencies suspected of failing to register under AML rules and imposing fines on others.[35] These efforts appear to be working and have decreased prices in London's top-end real estate market as agents and other industry professionals increasingly comply with AML regulations.[36]

## Criminal Money Laundering Exposures for Real Estate Professionals

### The Money Laundering Statutes

Beyond any purely regulatory duties, professionals involved in real estate transactions cannot disregard the U.S. federal criminal money laundering statutes, which may apply in extreme cases.

Very generally, the offence of money laundering under 18 U.S.C. §§ 1956 or 1957 involves a financial transaction conducted with the proceeds of a "specified unlawful activity", or "SUA", while knowing that the proceeds were earned through illegal activity. The list of potential SUAs identified by Congress is specific but also extremely long (over 200 separate crimes).[37] As a practical matter it encompasses almost any conceivable crime. Further, Section 1956 generally also requires the defendant to act with one of four possible intents: an intent to conceal or disguise the nature, location, source, ownership or control of the SUA proceeds; to promote the underlying SUA; to avoid a transaction reporting requirement, such as a SAR; or to commit the offence of tax evasion or filing a false tax return. However, Section 1957 – the so-called "spending" money laundering statute – merely requires a transaction involving over $10,000 and knowledge that the proceeds were derived from criminal activity. Section 1957 is incredibly broad and can apply to any transaction, no matter how mundane and even in the absence of any effort at concealing the transaction – so long as SUA proceeds over $10,000 were involved, and knowledge existed.

### Knowledge: the Key Element

Typically, the key element in money laundering cases focused on a third-party professional – *i.e.*, the real estate agent, lawyer, accountant, banker, merchant or other professional who had no direct involvement in committing the underlying SUA but who later assisted the person who committed the underlying SUA with subsequent financial transactions involving the resultant proceeds – is knowledge. *I.e.*, when the real estate professional helped the client acquire a property, did he or she know that the funds used to purchase the property (or pay rent) came from illegal activity?

When contesting the existence of knowledge, the professional may claim to have relied in good faith upon misinformation from others, and/or to have been so removed from events that he or she never learned the pertinent facts. As a result, the doctrine of "deliberate ignorance" or "willful blindness" has been instrumental in the government's success in many of these prosecutions. Under this doctrine, a professional may be found to have guilty knowledge (here, that the proceeds derived from an SUA) if the defendant knew of a high probability that a transaction involved tainted funds and deliberately avoided learning the truth. The doctrine of willful blindness represents a powerful tool for the government, particularly in regards to third-party professionals. Prosecutors successfully have used the willful blindness doctrine to convict real estate agents,[38] lawyers, accountants, bankers, and other professionals of assisting in financial transactions involving the proceeds of schemes performed by others, despite the fact that the professionals had no involvement in the underlying SUAs.

Of course, sometimes a real estate professional is directly involved in the SUA – not surprisingly, numerous mortgage fraud prosecutions involve defendants who are real estate professionals charged with both the underlying fraud and money laundering.[39] There, knowledge is much more clear, and the main issue usually is whether the underlying criminal scheme actually occurred.

### International Real Estate Transactions

High-end real estate transactions often involve buyers, funds and activity located outside of the U.S. Simply put, the money laundering statutes are broad and often can apply to such situations, including when the alleged SUA providing the dirty money occurs entirely abroad. Section 1956 defines "SUA" in part to specifically include a range of foreign offences, including bribery and public corruption, so long as the resulting financial transaction at issue was conducted in whole or in part in the United States.[40] Moreover, Section 1956(f) extends jurisdiction over extraterritorial conduct when "the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States", and the transaction has a value exceeding $10,000.[41] Thus, Section 1956(f) applies to *financial transactions* which occur in whole or in part in the U.S.; it does not require physical presence in the U.S. Likewise, "conduct" occurring in the U.S. is not limited solely to physical activity; electronic conduct, such as a wire transfer into the U.S. from abroad, might satisfy Section 1956(f) and provide U.S. prosecutors with jurisdiction.

Finally, the international transfer of funds can itself represent money laundering. Section 1956 contains a separate prong that prohibits "international" money laundering that applies to transportations or transfers of funds in or out of the United States. This prong contains three alternative intent requirements: (i) an intent to promote an SUA; (ii) knowledge that the transaction is designed to conceal the proceeds of an SUA; or (iii) knowledge that the transaction is designed to avoid a transaction reporting requirement.[42] Although the statute is not a model of clarity, it arguably does not even require the funds involved in the transaction to be actual SUA funds.[43]

## Forfeiture and Real Estate

Complementing the criminal sanctions applicable to money laundering offences, 18 U.S.C. § 981 sets forth a powerful tool for sanctioning money laundering violations by subjecting property traced to both domestic and international criminal offences to civil forfeiture to the United States.[44] Specifically as to domestic money laundering offences, it subjects to forfeiture "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title [described above], or any property traceable to such property."[45] Concerning international offences, the statute reaches "[a]ny property, real or personal, within the jurisdiction of the United States, constituting, derived from, or traceable to, any proceeds obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense" involves violations of the Controlled Substances Act, constitutes a felony in the foreign jurisdiction or constitutes a felony in the United States.

Civil forfeiture enables the government to achieve multiple enforcement aims through a single process. First, forfeiture enables the government to recoup potentially massive sums of illicitly laundered gains. Second, it often serves as high-profile examples of the government's enforcement reach and capabilities, contributing significantly to the government's deterrent efforts.

Recent examples illustrate the effectiveness of civil forfeiture proceedings to combat illicit laundering. In November 2019, the Justice Department settled a civil forfeiture action against assets acquired by Low Taek Jho and his family stemming from their alleged misappropriation from 1MDB, which they laundered through financial institutions around the world, including in the United States, Switzerland, Singapore and Luxembourg. As part of that settlement, Jho and the other defendants agreed

to the forfeiture of $700 million in assets, including high-end real estate in Beverly Hill, New York City and London; a luxury boutique hotel in Beverly Hills; and tens of millions of dollars in business investments.[46] In June 2017, the federal government obtained dual verdicts against 650 Park Avenue, a 36-story building in Manhattan, valued at up to $1 billion the government traced to Iranians convicted of violating American sanctions and money laundering statutes.[47]

## Endnotes

1. *See* FIN-2017-A003 (Aug. 22, 2017), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a003.
2. *E.g.* Kenneth Blanco, Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement (June 12, 2019), *available at* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and.
3. 31 C.F.R. § 1010.230.
4. *E.g.* Beth Moskow-Schnoll, Priya Roy, and Peter D. Hardy, *Money Laundering Watch*, Senate Committee Hears from OCC, FinCEN and FBI on Risks Posed by Anonymous Corporate Structures, *available at* https://www.moneylaunderingnews.com/2019/05/senate-committee-hears-from-occ-fincen-and-fbi-on-risks-posed-by-anonymous-corporate-structures/#more-5050.
5. U.S. Department of Treasury, National Strategy for Combating Terrorist and Other Illicit Financing (Feb. 6, 2020) *available at* https://home.treasury.gov/news/press-releases/sm902.
6. FATF, Mutual Evaluation Report on the United States' Measures to Combat Money Laundering and Terrorist Financing (Dec. 1, 2016), *available at* https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html.
7. 31 U.S.C. § 5312(a)(2)(u).
8. As discussed *infra* in the text, FinCEN has issued regulations covering certain nonbank residential mortgage lenders and originators. *See* 31 C.F.R. § 1010.00(lll)(1).
9. *See* FinCEN, FinCEN Reissues Real Estate Geographic Targeting Orders for 12 Metropolitan Areas (Nov. 8, 2019), *available at* https://www.fincen.gov/news/news-releases/fincen-reissues-real-estate-geographic-targeting-orders-12-metropolitan-areas-0.
10. *Id.*
11. 31 U.S.C. § 5312(a)(2)(p).
12. 74 Fed. Reg. 35,830 (July 21, 2009).
13. 77 Fed. Reg. 8148-8160 (Feb. 14, 2012).
14. 31 C.F.R. § 1010.100(lll)(1).
15. 68 Fed. Reg. 17,569 (April 10, 2003). However, all real estate professionals must follow their reporting obligations with regards to the Form 8300: a filing required under both the BSA and Internal Revenue Code, generally when a person receives over $10,000 in currency in the course of his or her trade or business. 31 U.S.C. § 5331.
16. *See* Senate Bill S.482, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/482.
17. DASKAA § 702(e)(1).
18. DASKAA § 702(e)(2)(A).
19. DASKAA § 702(e)(2)(C).
20. *See* Senate Bill S.2563, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2563?q=%7B%22search%22%3A%5B%22The+Improving+Laundering+Laws+and+Increasing+Comprehensive+Information+Tracking+of+Criminal+Activity+in+Shell+Holdings%22%5D%7D&s=6&r=1.
21. *Available at* https://www.congress.gov/bill/116th-congress/house-bill/2513.
22. *Forbes*, "British Real Estate Agents Hit By Money Laundering Crackdown" (March 11, 2019), *available at* https://www.forbes.com/sites/oliverwilliams1/2019/03/11/british-real-estate-agents-hit-by-money-laundering-crackdown/#614250463c88.
23. Transparency International UK, "Faulty Towers: Understanding the impact of overseas corruption on the London property market" (March 2017) ("Faulty Towers"), *available at* https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market/. FATF defines a PEP as an "an individual who is or has been entrusted with a prominent function". Because of their positions of power and access to large budgets, PEPs are considered high money laundering risk individuals. *Id.*
24. *Id.*
25. *Forbes*, "The London Property Deal That Brought Down Pakistan's Prime Minister" (Aug. 1, 2017), *available at* https://www.forbes.com/sites/bisnow/2017/08/01/the-london-property-deal-that-brought-down-pakistans-prime-minister/#2676fcd51942.
26. *WSJ*, "Stepson of Malaysia's Najib Razak Bought $34 Million London House With 1MDB Funds" (May 19, 2016), *available at* https://www.wsj.com/articles/stepson-of-malaysias-najib-razak-bought-34-million-london-house-with-1mdb-funds-1463634207.
27. For more examples, *see, e.g.*, National Crime Agency, Money laundering and illicit finance, *available at* https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing.
28. Faulty Towers, *supra* at n. 23. A recent investigation using information obtained from freedom of information legislation revealed that the HMRC – a supervisory body for AML regulations – has conducted less than 55 investigations of real estate agents into breaches of their AML obligations. *See Wired*, "New data shows London's property boom is a money laundering horror" (April 9, 2019), *available at* https://www.wired.co.uk/article/money-laundering-hmrc-tax-update.
29. Faulty Towers, *supra* at n. 23.
30. Anti-Corruption Summit – London 2016 UK Country Statement (May 2016), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522749/United_Kingdom.pdf.
31. UK.gov, "A register of beneficial owners of overseas companies and other legal entities: potential impacts" (July 23, 2018), *available at* https://www.gov.uk/government/publications/a-register-of-beneficial-owners-of-overseas-companies-and-other-legal-entities-potential-impacts.

32. HMRC, "Estate agency guidance for money laundering supervision" (May 1, 2019), *available at* https://www.gov.uk/government/publications/money-laundering-regulations-2007-supervision-of-estate-agency-businesses/estate-agency-guidance-for-money-laundering-supervision. *See also Financial Times*, "UK estate agents hit by crackdown on money laundering" (March 9, 2019), *available at* https://www.ft.com/content/15ef0b06-40cd-11e9-b896-fe36e-c32aece.
33. Gov.uk, "Circular 003/2018: unexplained wealth orders" (Jan. 31, 2018), *available at* https://www.gov.uk/government/publications/circular-0032018-criminal-finances-act-unexplained-wealth-orders/circular-0032018-unexplained-wealth-orders?mod=article_inline.
34. *See Independent*, "Investigators probe £80m London properties linked to 'politically exposed person involved in serious crime'" (May 29, 2019), *available at* https://www.independent.co.uk/news/uk/crime/london-money-laundering-unexplained-wealth-orders-mcmafia-a8933866.html.
35. *Financial Times*, "UK estate agents hit by crackdown on money laundering" (March 9, 2019), *available at* https://www.ft.com/content/15ef0b06-40cd-11e9-b896-fe36e-c32aece.
36. *Id.* For example, a pending London home purchase for £100 million collapsed in 2018 because the lender was not satisfied about the source of the buyer's funds. *Id.*
37. 18 U.S.C. § 1956(c)(7).
38. *See United States v. Nguyen*, 493 F.3d 613, 619-22 (5th Cir. 2007); *United States v. Campbell*, 977 F.2d 854, 858-59 (4th Cir. 1992).
39. *E.g. United States v. Catarro*, 746 Fed. Appx. 110, 112-15 (3d Cir. 2018); *United States v. Cox*, 851 F.3d 113 (1st Cir. 2017).
40. 18 U.S.C. § 1957(c)(7)(B).
41. 18 U.S.C. § 1956(f).
42. 18 U.S.C. § 1957(a)(2).
43. Peter D. Hardy, Criminal Tax, Money Laundering and Bank Secrecy Act Litigation Ch. 3.III.C (BNA Bloomberg 2010).
44. 18 U.S.C. § 981(a).
45. 18 U.S.C. § 981(a)(1)(A).
46. *See* Stipulation and Request to Enter Consent Judgment of Forfeiture, *United States v. Any Rights to Profits, Royalties and Distribution Proceeds Owned by or Owed Relating to EMI Music Publishing Group* (C.D. Cal. Oct. 30, 2019), *available at* https://www.justice.gov/opa/press-release/file/1214051/download.
47. *See* Press Release No. 17-200, Acting Manhattan U.S. Attorney Announces Historic Jury Verdict Finding Forfeiture of Midtown Office Building and Other Properties (June 29, 2017), *available at* https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-historic-jury-verdict-finding-forfeiture-midtown.

**Peter D. Hardy** is a partner at Ballard Spahr LLP. He leads the firm's Anti-Money Laundering ("AML") Team, and advises financial institutions on Bank Secrecy Act ("BSA") compliance. He also defends companies and individuals against allegations of misconduct and related civil litigation. Peter co-chairs the Practising Law Institute's AML programme, and is the author of *Criminal Tax, Money Laundering, and Bank Secrecy Act Litigation*, a legal treatise published by Bloomberg BNA. Peter edits *Money Laundering Watch*, Ballard's blog on money laundering issues. Peter previously spent over a decade as a federal prosecutor.

**Ballard Spahr LLP**
1735 Market Street, 51st Floor
Philadelphia, PA 19103-7599
USA

Tel: +1 215 864 8838
Email: hardyp@ballardspahr.com
URL: www.ballardspahr.com

**Terence M. Grugan** is of counsel practising in Ballard Spahr's White Collar Defense/Internal Investigations and Securities Enforcement and Corporate Governance Litigation practice groups. As part of the firm's AML Team, he advises clients on issues arising under the BSA and defends clients in matters implicating AML compliance obligations. He also represents individuals and corporations in government investigations and securities-related investigations and litigation.

**Ballard Spahr LLP**
1735 Market Street, 51st Floor
Philadelphia, PA 19103-7599
USA

Tel: +1 215 864 8320
Email: grugant@ballardspahr.com
URL: www.ballardspahr.com

**Priya Roy** is an associate in Ballard Spahr's White Collar Defense/Internal Investigation and Securities Enforcement and Corporate Governance Litigation practice groups, and the AML Team. She focuses her practice on complex business and regulatory litigation and regularly advises clients on issues arising under the BSA. Priya specifically counsels real estate industry clients on AML and money laundering issues, and advises on civil discovery and expert testimony issues relating to the BSA. She also represents individuals and corporations in government investigations and securities-related audits and investigations.

**Ballard Spahr LLP**
1735 Market Street, 51st Floor
Philadelphia, PA 19103-7599
USA

Tel: +1 215 864 8336
Email: royp@ballardspahr.com
URL: www.ballardspahr.com

**Mary K. Treanor** is an associate in Ballard Spahr's Litigation Department, White Collar Defense/Internal Investigations group, and AML Team. She focuses her practice on white collar defence and complex commercial and regulatory litigation. She advises clients on BSA and AML matters, including government and internal investigations. She also counsels financial institutions on Suspicious Activity Report filings and confidentiality requirements.

**Ballard Spahr LLP**
1735 Market Street, 51st Floor
Philadelphia, PA 19103-7599
USA

Tel: +1 215 864 8131
Email: treanorm@ballardspahr.com
URL: www.ballardspahr.com

Ballard Spahr LLP is a national firm of more than 650 lawyers in 15 offices across the United States. Our attorneys provide counselling and advocacy in more than 50 areas within business and transactions, finance, intellectual property, litigation, and real estate. We represent a diverse cross-section of clients, ranging from large public companies and privately held entities to government bodies and nonprofit organisations. Our practices span the financial, industrial, real estate, private equity, retail, and other sectors that are critical to growth in today's marketplace. Ballard's AML Team advises a broad range of financial institutions – including banks, money services businesses, casinos, residential mortgage originators and lenders, and others – on BSA/AML compliance. The AML Team further represents financial institutions in government examinations, audits and enforcement proceedings, as well as civil litigation alleging underlying violations of the BSA.

**www.ballardspahr.com**

Ballard Spahr LLP

# EU Legislation in the Area of AML: Historical Perspective and *Quo Vadis*

Linklaters LLP

Stefaan Loosveld

## Introduction

Since the EU adopted its first legislation in the area of anti-money laundering ("AML") in 1991,[1] the EU legislator has, over the years, become increasingly active.

This activity mainly concerns the expansion of the entities and activities covered by AML requirements, the increase of the nature and scope of these requirements, and the strengthening of the powers of the competent authorities in the area of AML.

The below overview summarises the development of the EU legislation in the area of AML since 1991 to date, and sketches what may lay further ahead.

## From 1991 to 2015: From the 1st to the 4th AML Directive

The 1st AML Directive dates from 1991 and remained unchanged for a decade.[2] It defined "money laundering" in terms of drugs-related offences and imposed obligations on the financial sector.

The 2nd AML Directive was adopted in 2001.[3] It extended the scope of the 1st AML Directive in terms of both the crimes and the range of professions and activities covered.

Four years later, in 2005, the 3rd AML Directive was adopted.[4] This directive reflected the revisions that the Financial Action Task Force ("FATF") had undertaken in June 2003, in the wake of the 9/11 terrorist attacks, of its recommendations in order to also cover terrorist financing and related offences. These recommendations included more detailed requirements in terms of customer identification and verification, situations where a higher risk of money laundering or terrorist financing could justify enhanced measures and, conversely, situations where a reduced risk could justify less rigorous controls. A number of measures implementing the 3rd AML Directive, amongst others as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures, were laid down in Directive 2006/70.[5]

The 4th AML Directive was adopted in 2015.[6]

This directive introduces a significant range of new rules compared to the previous three directives. Amongst others, it lays down the obligation for the EU Member States to create a centralised register of so-called "Ultimate Beneficial Owners" ("UBOs"), with detailed information on the legal entities registered in EU Member States. Another change introduced by the 4th AML Directive is the risk-based approach. This requires obliged entities to demonstrate improved methods of conducting risk assessments to identify and assess their AML-related risks.

The 4th AML Directive replaces the previous three EU directives. Hence, since 2015, the main piece of EU legislation in the area of AML is the 4th AML Directive, as amended thereafter from time to time. To date, these amendments are the 5th AML Directive, which was adopted in 2018 (see below), and Directive 2019/2177, which was adopted in 2019 (see below).

## 2018: The 5th AML Directive

The 5th AML Directive was adopted on 30 May 2018.[7] It brings about a number of changes to the 4th AML Directive. It entered into force on 9 July 2018 and the EU Member States had to implement it in their respective national laws by 10 January 2020.[8]

The overall aim of the 5th AML Directive is to overcome three perceived gaps for the effectiveness of the EU's efforts in the area of AML:[9]

- gaps created by increasing advances in technology and communications, coupled with the globally interconnected financial system;
- gaps in the oversight of the manifold financial means that can be used for illegitimate activities, while at the same time avoiding that new EU legislation would raise unnecessary obstacles to the functioning and development of payments and financial markets for legitimate activities; and
- gaps in the transparency of financial transactions around the world, with offshore jurisdictions being often used as locations of intermediary entities that distance the real, beneficial owner from the assets owned.

To this effect, the 5th AML Directive brings about a number of changes to the 4th AML Directive. The main changes are the following:

- Increasing the investigatory powers of the FIUs,[10] particularly in terms of access to, and exchange of, information. To this effect, the 5th AML Directive provides for the obligation of the EU Member States to set up automated registers or data retrieval systems allowing for the identification of the holders of bank and payment accounts, and to which the FIUs or other competent authorities can have access.
- Increasing the transparency regimes for information on the beneficial owners of legal entities (companies, trusts and similar legal arrangements). To this effect, the national UBO registers become publicly accessible[11] and are interconnected with each other, so that foreign information can be accessed as well.[12]
- Enhancing the due diligence measures that obliged entities have to apply with regard to high-risk third countries,[13] through a combination of a prescriptive list of such measures and an illustrative list of countermeasures that could be applied when dealing with high-risk countries that are designated by the EU Commission.

- Enabling competent authorities to monitor suspicious transactions with virtual currencies, while preserving the innovative advances offered by such currencies.

With respect to this last change, under the regime before the 5th AML Directive, providers of exchange services between virtual currencies and fiat currencies as well as custodian wallet providers did not qualify as obliged entities for AML purposes. Accordingly, they did not have an obligation to identify suspicious activity.

However, as the 5th AML Directive highlights, the anonymity of virtual currencies allows their potential misuse for criminal purposes.[14] Particularly the global reach and complex, cross-border technology and communications infrastructure of virtual currencies is relevant in this respect, as components of a virtual currency system may be located in jurisdictions that do not have an adequate AML regime.

Addressing these risks is the main stated reason that the 5th AML Directive now also designs such exchange services and wallet providers as obliged entities.[15] Henceforth, they also have a registration obligation.[16] In addition, the respective competent authorities in the EU Member States for these entities need to ensure that the persons who hold management functions in them, or are their beneficial owners, are fit and proper.[17] In order to give meaning to these obligations, the 5th AML Directive contains a number of definitions, including that of "*virtual currencies*".[18]

While the 5th AML Directive thus submits virtual currencies and their providers to a number of legal and regulatory requirements, the applicable AML regime is not as far-reaching as the one that traditionally exists.

For instance, the 5th AML Directive does not introduce an obligation for EU Member States to set up and maintain a central database registering the identities of the issuers and the wallet addresses, and to which the FIUs could have access. The directive only provides that the future report that the European Commission will need to draw up and publish by 11 January 2022 on the implementation of this directive shall be accompanied, "*if necessary, by appropriate legislative proposals, including, where appropriate*" on issues regarding virtual currencies. These issues will, for instance, consider whether or not such central database should be set up, and whether or not the users of virtual currencies should have the possibility to self-declare to designated authorities.[19]

The stated rationale behind the reluctance of the EU legislator to submit the use of virtual currencies to requirements that are too strict – i.e. the "balanced and proportional approach" in the words of the 5th AML Directive[20] – is that the legislator does not wish to stifle technical advance and innovation, particularly in the technology that underlies virtual currencies, such as blockchain and the so-called "distributed ledger technology" or "DLT".[21]

Besides the AML concerns addressed in the 5th AML Directive, the use and further growth of virtual currencies also raises a number of other legal and regulatory considerations, which often touch upon FinTech generally.

For instance, the newly designated obliged entities will have to collect and process personal data (i.e. by performing customer due diligence) and will, as a consequence, have to abide by the relevant data protection obligations, such as the General Data Protection Regulation ("GDPR") in the EU.

Licensing and related issues might also arise if entities that are, directly or indirectly, involved in transactions with virtual currencies exercise, through this involvement, regulated activities. As an example, if such activities qualify as the provision of payment services in the EU, due regard will need to be given to the EU's Second Payment Services Directive ("PSD 2").[22]

Other regulatory considerations touch upon consumer protection, cross-border capital flow management (such as exchange controls and sanctions legislation) and taxation.[23]

## 2018: The AML-Criminal Directive

Following the adoption of the 5th AML Directive, the EU focused its work on two new pieces of EU legislation in the area of AML.

The first piece aims to strengthen the EU supervisory framework for the financial sector by giving increased regulatory powers to the European Banking Authority in the area of AML. It has led to the adoption at the end of 2019 of a new EU directive (see below).

The second concerns the introduction of EU-wide rules on the criminalisation of money laundering conduct through the adoption of the AML-Criminal Directive on 23 October 2018.[24] The EU Member States must have transposed this directive into their respective national laws by 3 December 2020 at the latest.[25]

The AML-Criminal Directive establishes common rules to criminalise certain types of money laundering conduct throughout the EU.

While a number of requirements for the criminalisation of money laundering have already existed in EU legislation since 2001, this legislation was seen as insufficiently comprehensive and coherent, and resulted in enforcement gaps and obstacles to cooperation between the competent authorities in the EU Member States.[26]

The EU legislator also saw the need for the adoption of common criminal rules in view of the new money-laundering risks and challenges presented by new technologies. The AML-Criminal Directive specifically refers in this context to the use of virtual currencies.[27]

The AML-Criminal Directive does not consist of a full harmonisation but only establishes a number of uniform minimum rules. It is nonetheless significant. For instance, it harmonises key criminal law provisions in terms of the substantive rules for the predicate offences, the conditions in which both individuals and legal entities can be held criminally liable, the criminal sanctions for the offences and some jurisdictional rules for prosecuting money-laundering conduct.

To this effect, the AML-Criminal Directive complements and reinforces by means of criminal law the 4th AML Directive.[28] It is not the first time that the EU legislator has strengthened, through EU criminal law rules, an existing EU regulatory framework. Another notable example is in the area of market abuse where the existing EU legislation was complemented in 2014 with the EU Directive 2014/57/EU on criminal sanctions for market abuse.[29]

## 2019: Regulation 2019/2175

Through various EU legislative instruments and actions, the EU has in the past decade not only significantly strengthened the AML framework under discussion in this chapter.

It has also fundamentally overhauled and reinforced the EU financial supervisory framework, particularly since the financial crisis of 2008. Key therein is the completion of the EU Banking Union, which consists of four pillars. The first two pillars place the banking system within the eurozone under the common responsibility of the Single Supervisory Mechanism ("SSM")[30] and the Single Resolution Mechanism ("SRM"),[31] effective as of 4 November 2014 and 1 January 2016, respectively.[32] The interaction between the EU financial supervisory framework and the EU AML framework raises, however, two key concerns.

First, how can it be ensured that both frameworks function, from a substantive viewpoint, coherently together, leading

to effective and robust AML in the financial sector? Second, what needs to be done institutionally to bolster this coherence in view of where the most important supervisory competencies and powers are currently located, i.e. largely at the national level for AML while largely centralised at the EU level for banking supervision (SSM). Amongst others, recent serious money-laundering cases in the EU revealed, according to the supervisors, a number of deficiencies in the current AML framework as applied to financial institutions, mainly related to the absence of an adequate cooperation between supervisors.

The wish to plug deficiencies that exist at the crossroads of the AML and the prudential supervisory frameworks is the reason for the adoption on 18 December 2019 of Regulation 2019/2175.[33] This regulation entered into force on 30 December 2019 and, as a rule, applies as from 1 January 2020.[34]

Regulation 2019/2175, amongst others, brings about a number of changes to the powers, decision-making and governance processes, supervisory priorities, budgetary and financial rules, and related institutional setup of the three European Supervisory Authorities ("ESAs") that were created in 2010, i.e. the European Banking Authority ("EBA"), the European Insurance and Occupational Pensions Authority ("EIOPA") and the European Securities and Markets Authority ("ESMA").[35]

To this effect, Regulation 2019/2175 amends a number of provisions in the existing legislation governing the three ESAs.[36] Importantly, these amendments will also change the existing ESAs legislation – mainly the EBA Regulation – to ensure that the EU's financial supervisory and AML frameworks effectively function together in terms of, on the one hand, the regulators that supervise both frameworks, and, on the other hand, the institutional level (EU or national) at which this supervision is carried out.

In view thereof, Regulation 2019/2175 centralises the tasks, expertise and resources related to AML at the EBA. It also reinforces the EBA's powers for carrying out AML-related tasks and strengthens the EBA's international role in this regard.

Regulation 2019/2175 further gives the power to the EBA, in AML matters and in accordance with the EU's AML Directives, where the EBA has indications of material breaches by a financial sector operator, to request a competent authority to investigate possible breaches and to consider imposing sanctions on that operator for such breaches. It grants a number of additional powers to the EBA, such as to adopt, under certain conditions, binding decisions in the area of AML that are addressed directly to financial sector operators.[37]

## 2019: Directive 2019/2177

The above-mentioned centralisation at the EBA of a wide range of AML-related tasks has also required a limited number of changes to the 4th AML Directive.

These changes have been introduced by Directive 2019/2177.[38] While this directive changes the 4th AML Directive, it also deals with a range of other issues that are unrelated to AML. Hence, it cannot really be viewed as the 6th EU Directive in the area of AML.

Directive 2019/2177 entered into force on 30 December 2019. The AML-related provisions need to be transposed in the national laws of the EU Member States by 30 June 2021.[39]

The changes that Directive 2019/2177 introduce to the 4th AML Directive mainly concern the power of the EBA to issue guidelines and develop draft regulatory technical standards regarding a number of AML matters, and the exchange of information between the EBA, the EU Commission, the EU Member States, the competent authorities in the area of AML and the financial supervisory authorities in the EU Member States.[40]

A noteworthy change is that the EU Member States will have to ensure that their competent authorities inform the EBA of all administrative sanctions and measures imposed on credit institutions and financial institutions for breaches of national provisions transposing the 4th AML Directive (as amended), including of any appeal in relation thereto and the outcome thereof. In the same context, the EBA will have to maintain a website with links to each competent authority's publication of such administrative sanctions and measures, and show the time period for which each Member State publishes administrative sanctions and measures.[41]

## 2020 and Beyond: A 6th AML Directive in the Making?

Even after the already significant legislative activity in 2018 and 2019, and notwithstanding the fact that a number of EU Member States have still not implemented the 5th AML Directive, the EU continues its legislative work in relation to AML.

Thus, on 12 February 2020, the EU Commission opened a consultation on a roadmap for an Action Plan on AML to be published by the end of March 2020.[42]

The Action Plan will focus on the cross-border aspects of AML and on addressing a number of further perceived gaps and vulnerabilities in the existing framework and which the Commission already highlighted in a report of 24 July 2019.[43] These include: (i) the application of the AML rules by professionals, particularly above and beyond financial institutions; (ii) supervision by national authorities; (iii) the functioning of the Financial Intelligence Units;[44] and (iv) the importance of ensuring that the AML regime is and remains fit for FinTech.

Based on the consultation and the outcome of discussions with all stakeholders, it is expected that the Commission will come with policy initiatives and legislative proposals in 2021, possibly leading to new EU legislation in the area of AML (whether or not in the form of a 6th AML Directive). This legislation could then possibly also include the creation of a specific AML supervisor at the EU level.

A second relevant development is the work undertaken by the EBA to update its 2017 Risk Factors Guidelines.[45] These Guidelines deal with customer due diligence ("CDD") and the factors that financial institutions should consider when assessing the money-laundering risk associated with individual business relationships and occasional transactions. They also set out how firms can adjust the extent of their CDD measures in a way that is commensurate to the risks they have identified. The EBA has recently published draft new guidelines in this area and launched a consultation regarding this draft with comments to be submitted by 5 May 2020.

The rationale for this new draft is that, since 2017, the EU legislative framework in the area of AML has changed and new risks have emerged. The 5th AML Directive (see above) has introduced a number of changes that warrant a review of the Risk Factor Guidelines to ensure their ongoing accuracy and relevance. This is particularly the case in relation to the provisions on enhanced CDD related to high-risk third countries. To support the AML compliance efforts of financial institutions and enhance the ability of the EU's financial sector to effectively deter and detect money laundering, the new draft guidelines update a number of issues, such as: (i) business-wide and individual money-laundering risk assessments; (ii) CDD measures including on the beneficial owner; (iii) terrorist-financing risk factors; and (iv) new guidance on emerging risks, such as the use of innovative solutions for CDD purposes.

As was the case previously, the new draft guidelines are divided into two parts. Title I is generic and applies to all firms. It is designed to equip firms with the tools they need to make informed, risk-based decisions when identifying, assessing and

managing money-laundering risks associated with individual business relationships or occasional transactions. Title II is sector specific and complements the generic guidelines in Title I.46. Together, Title I and Title II promote the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML entails and how it should be applied.

## Note

This chapter reflects the personal views of the author and not of Linklaters. It does not contain legal advice.

## Endnotes

1. In what follows and unless indicated otherwise, references to AML include CTF ("countering terrorism financing").
2. In full: Directive 91/308 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77.
3. In full: Directive 2001/97 amending Directive 91/308 on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76.
4. In full: Directive 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15.
5. In full: Directive 2006/70 laying down implementing measures for Directive 2005/60 as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis [2006] OJ L214/29 (as amended by the Directive 2008/20 amending Directive 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as regards the implementing powers conferred on the Commission [2008] OJ L76/46).
6. In full: Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation 648/2012, and repealing Directive 2005/60 and Directive 2006/70 [2015] OJ L141/73.
7. In full: Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43. See on the 5th AML Directive: S. Loosveld, *The 5th EU Anti-Money Laundering Directive: Virtual Currencies and Other Novelties*, [2018], J.I.B.L.R. 33, 297–304.
8. See Article 5 of the 5th AML Directive for the date of its entry into force and Article 4(1) for the date of its transposition into national law.
9. See Explanatory Memorandum COM(2016) 450 final of 5 July 2016.
10. FIUs are the so-called "EU Financial Intelligence Units", i.e. the operationally independent and autonomous central unit that each EU Member State has established in order to prevent, detect and effectively combat money laundering and terrorist financing. An FIU is responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, terrorist financing and associated predicate offences, and for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect such offences.
11. See, amongst others, Article 1(15)(c) and Article 1(16)(d) of the 5th AML Directive, which replace, respectively, Article 30, 5th paragraph and Article 31, 4th paragraph of the 4th AML Directive. The conditions for such access, and the level of information obtained through such access, depend, amongst others, on whether the request is made by competent authorities and FIUs, obliged entities, or members of the general public. There exists, in certain circumstances, the possibility for a case-by-case exemption from such access to all or part of the information on the beneficial ownership.
12. This interconnection will need to be transposed into national law by 10 March 2021 at the latest.
13. Article 9(1) of the 4th AML Directive defines "High-risk third countries" as "*third-country jurisdictions [i.e. not EU Member States] which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the [European] Union*".
14. See whereas (9) of the 5th AML Directive.
15. See Article 1(1)(c) of the 5th AML Directive, which includes, through the new Articles 2(1)(3)(g) and (h) of the 4th AML Directive, in the list of obliged entities "*the providers engaged in exchange services between virtual currencies and fiat currencies*" (see (g)) and "custodian wallet providers" (see (h)). As these new provisions are part of the list of obliged entities in Article 2(1)(3) of the 4th AML Directive, the providers concerned only qualify as "obliged entities" if they are "*natural or legal persons acting in the exercise of their professional activities*".
16. See Article 1(29) of the 5th AML Directive, which replaces Article 47(1) of the 4th AML Directive.
17. See Article 47(2) of the 4th AML Directive, which refers to the entities referred to in Article 47(1) thereof and which, by virtue of Article 1(29) of the 5th AML Directive, now also includes exchange platforms and custodian wallet providers.
18. See Article 1(2)(d) of the 5th AML Directive, which inserts this definition in the new Article 3(19) of the 4th AML Directive.
19. See Article 1(41) of the 5th AML Directive, which contains the new Article 65(1), last paragraph, of the 4th AML Directive.
20. See whereas (8), last sentence, of the 5th AML Directive.
21. The term DLT is used in the financial industry in a variety of ways and without a single definition. It is, generally speaking, understood as a technology that combines a number of components, such as peer-to-peer networks, distributed data storage and cryptography, and that allows for the storage and keeping of records and transfer of digital assets (e.g. virtual currencies) in an operationally more efficient and cost-effective manner (see e.g. D. Mills *et al.*, "Distributed ledger technology in payments, clearing, and settlement", Finance and Economics Discussion Series 2016-095, Washington, Board of Governors of the Federal Reserve System, 3; A. Pina and W. Ruttenberg, "Distributed ledger technologies in securities post-trading. Revolution or Evolution?", ECB Occasional Paper Series, No. 172, April 2016, 8 and following).
22. In full: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35.
23. See e.g. for the EU regulatory framework: European Parliament, TAX3 committee, "Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion", Brussels, July 2018.

24. In full: Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L 284/22. See for the main features of the AML Criminal Directive, S. Loosveld, *The New EU Directive on Combating Money Laundering by Criminal Law* [2019] I.C.C.L.R. 168.
25. See Article 13(1) of the AML-Criminal Directive. The AML-Criminal Directive is not applicable to Denmark, Ireland and the UK (see whereas (23) and (24)).
26. See whereas (4) of the AML-Criminal Directive. The existing legislation is Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime [2001] OJ L 182/1.
27. See whereas (6) of the AML-Criminal Directive.
28. See whereas (1) of the AML-Criminal Directive.
29. In full: Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive) [2014] OJ L 173/179.
30. The SSM consists of the European Central Bank ("ECB") and the national competent authorities for supervising credit institutions and (mixed) financial holding companies in the Eurozone. The ECB is responsible for the effective and consistent functioning of the SSM. It is exclusively competent for a wide range of significant prudential supervisory tasks, such as authorising and withdrawing the authorisation of supervised entities, assessing the acquisition and disposal of holdings therein, and ensuring compliance with EU and national legislation on prudential requirements in key areas, such as own funds, liquidity, leverage, large exposures, capital adequacy and robust governance. Among the thousands of supervised entities that are established in the euro area, the ECB has full and direct supervisory authority over so-called "significant institutions". The national supervisory authorities are, on the one hand, responsible for assisting the ECB in the preparation and implementation of the ECB's exercise of its supervisory tasks – including the ongoing day-to-day assessment of an institution's situation – and, on the other hand, remain competent in the areas not covered by the SSM.
31. The SRM consists of the Single Resolution Board ("SRB"), established in Brussels, and the national resolution authorities of the Eurozone Member States. Institutions whose home supervisor is the ECB or the national supervisory authority in the Eurozone Member States are, for resolution purposes, subject to the SRB or the national resolution authority in these Member States. As with the SSM, the SRM also contains a division of tasks between the SRB and the national resolution authorities that are part of the SRM. The SRB is responsible for the effective and consistent functioning of the SRM as well as for drawing up resolution plans and adopting resolution-related decisions with regard to the same significant institutions in the Eurozone that the ECB directly supervises in the framework of the SSM. With a number of exceptions (notably non-significant cross-border banking groups that are established in the Eurozone and for which the SRB is also directly responsible), the national resolution authorities are responsible for resolution planning and decisions with regard to the other Eurozone institutions.
32. The two other pillars of the banking union are a single rulebook for financial services in the EU and a European deposit insurance scheme. The single rulebook already consists of an impressive body of EU legislation, which is regularly updated and complemented. Work on establishing the deposit insurance scheme is still ongoing and subject to important policy discussions regarding its key features and the budgetary implications of such schemes for EU Member States.
33. In full: Regulation (EU) 2019/2175 of the European Parliament and of the Council amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority); Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority); Regulation (EU) No 600/2014 on markets in financial instruments; Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds; and Regulation (EU) 2015/847 on information accompanying transfers of funds [2019] OJ L334/1. See for the main features of Regulation 2019/2175: S. Loosveld, *The EU Regulation 2019/2175 and the Strengthening of the EU Supervisory Framework in the Area of AML* [2020], J.I.B.L.R. 35, 115–121.
34. See Article 7 of Regulation 2019/2175.
35. To illustrate a number of the novelties generally brought about by Regulation 2019/2175 that go beyond the specific AML context – the three ESAs will: need to set up whistle-blowing type reporting channels (see e.g. Article 17(a) of the EBA Regulation); have the competence to issue opinions on all issues related to their respective area of competence (see e.g. Article 16(a) of the EBA Regulation); and have a web-based tool for handling Q&As (see e.g. Article 16(b) of the EBA Regulation). Besides the EU legislation regarding the ESAs generally, Regulation 2019/2175 also brings about a number of changes to other EU sectoral legislation. Thus, it significantly increases the investigatory and sanctioning powers of ESMA under MiFIR (Regulation (EU) No 600/14 on markets in financial instruments and amending Regulation (EU) No 648/2012 [2014] OJ L173/84) and under the Benchmarks Regulation (Regulation (EU) No 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investments funds amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 [2016] OJ L171/1).
36. I.e. Regulation 1093/2010 as regards the EBA (in full: Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC [2010] OJ L331/12), Regulation 1094/2010 as regards EIOPA (in full: Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC [2010] OJ L331/48) and Regulation 1095/2010 as regards ESMA (in full: Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC [2010] OJ L331/84).

37. This term refers to an entity that is subject to the 4th AML Directive (as amended) and that is either a "financial institution" for the purposes of the EBA or EIOPA Regulations, or a "financial market participant" for the purposes of the ESMA Regulation. This definition ensures that institutions that are supervised by each of the three ESAs are captured.
38. In full: Directive (EU) 2019/2177 of the European Parliament and of the Council of 18 December 2019 amending Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Directive 2014/65/EU on markets in financial instruments and Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing [2019] OJ L334/155.
39. See Article 5 (entry into force) and Article 4 (transposition) of Directive 2019/2177.
40. See Article 3(1) to (9) of Directive 2019/2177, which amends or replaces to this effect a number of provisions in the 4th AML Directive.
41. See Article 3(10) of Directive 2019/2177, which amends to this effect Article 62 of the 4th AML Directive.
42. Whereas, in the past, the Commission's work on AML was led by the Directorate-General ("DG") Justice, this new action will be led by the DG for Financial Stability, Financial Services and Capital Markets Union ("Fisma").
43. See the Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM(2019) 370 final). This is one of the four reports on AML that the Commission published on 24 July 2019; the other three are: (i) the Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units (COM(2019) 371 final); (ii) the Report from the Commission to the European Parliament and the Council on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts (COM(2019) 372 final); and (iii) the Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money-laundering cases involving EU credit institutions (COM(2019) 373 final).
44. See above, endnote 10, for these FIUs.
45. The 2017 Risk Factors Guidelines have been adopted under Articles 17 and 18(4) of the 4th AML Directive of 2017 and jointly issued by the three ESAs (see https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf). The new draft guidelines have been developed by the Joint Committee of the three ESAs. However, since the entry into force of Regulation 2019/2175 on 1 January 2020, ESMA and EIOPA no longer have direct responsibility for AML (see above). Therefore, only the EBA has launched the consultation.
46. Thus, Title 2 sets out risk factors that are of particular importance in certain of those sectors and provides guidance on the risk-sensitive application of CDD measures by firms in those sectors. To foster greater convergence of supervisory expectations of the measures firms should take to tackle emerging risks, additional sectoral guidelines have been added to the original Risk Factors Guidelines on crowdfunding platforms, providers of currency exchange services, corporate finance, and payment initiation services providers ("PISPs") and account information service providers ("AISPs"). Therefore, Title II now contains in total 13 sectoral guidelines about very different key financial sectors such as, for instance, correspondents banking, retail banking, electronic money, money remittance, life insurance and investments firms.

**Stefaan Loosveld** has been a partner at Linklaters since 2012, specialising in litigation (including white-collar), contentious regulatory and restructuring and insolvency (including sovereign default and debt restructuring). He acts for both financial institutions and corporates in complex litigation and arbitration matters.

**Linklaters LLP**
Rue Brederode 13
Brussels 1000
Belgium

Tel: +32 2 501 94 11
Email: stefaan.loosveld@linklaters.com
URL: www.linklaters.com

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


Dennis Miralis


Phillip Gibson

Nyman Gibson Miralis

## Introduction

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

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

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

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

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

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

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

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

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

Between 18–23 August 2019, Australia hosted the 2019 APG annual meeting and technical assistance forum, which was held in Canberra and led by Deputy Commissioner Close and Mr Abu Hena Mohammad Razee Hassan. This represented the 22nd consecutive annual meeting of APG members. The 2020 meeting will be hosted in Bangladesh.[2]

On 7 and 8 November 2019, Australia also hosted the 2nd annual 'No Money for Terror' Ministerial conference, which was held in Melbourne and led by the Hon. Peter Dutton, Minister for Home Affairs. Sixty-five delegations attended the event, at which focused sessions were held on emerging terrorist threats and terrorist-financing methods. The 2020 meeting will be hosted in India.[3]

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

The APG mutual evaluations or 'peers review' process involves site visits conducted by rotating teams consisting of APG legal, financial and law enforcement experts. These teams attend upon the jurisdiction of fellow APG members for the purpose of testing their levels of technical compliance with AML standards, as set by the FATF, as well as anti-money laundering and counter-terrorism financing effectiveness.[4]

A recent example of the mutual evaluation process was the APG on-site visit conducted between 4–15 November 2019 at Hanoi and Ho Chi Minh City, Vietnam. The APG mutual evaluation team on this occasion consisted of:

1. Mr Sok Heng Hak, Legal Assessor, Cambodia.
2. Mr Duarte Chagas, Legal Assessor, Macao, China.
3. Ms Zhang Yi, Financial Assessor, China.
4. Mr Ahmad Farhan, Financial Assessor, Malaysia.
5. Mr Jesse Baker, Financial Assessor, United States.
6. Mr Nesar Ahmad Yosufzai, FIU/Law Enforcement Assessor, Afghanistan.
7. Mr Daniel Burnicle, FIU/Law Enforcement Assessor, Australia.

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

The on-site visit was facilitated by the APG secretariat who met with H.E. Mr Vuong Dinh Hue, Deputy Prime Minister of Vietnam. The findings of this mutual evaluation process will be published in a report and presented at the 23rd APG annual meeting, which is to occur in Dhaka, Bangladesh in July 2020.[5]

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

1. Australia.
2. Malaysia.
3. Samoa.
4. Sri Lanka.
5. Vanuatu.
6. Canada.
7. Singapore.
8. Bangladesh.
9. Bhutan.
10. United States.
11. Cambodia.
12. Mongolia.
13. Macao, China.
14. Thailand.
15. Palau.
16. Cook Islands.
17. Indonesia.
18. Myanmar.
19. Fiji.
20. Chinese Taipei.
21. Pakistan.
22. Solomon Islands.[6]

Further to intergovernmental collaboration, the APG has also expressly provided for an increased strategic focus on information sharing and education with private sector agencies under the APG's private sector outreach programme.[7]

The FATF and the APG also conduct joint mutual evaluations to assess the AML/CTF regime of member jurisdictions against the international standards set by the FATF. On 4 September 2019, the FATF published the Mutual Evaluation Report on Hong Kong, following an on-site visit by FATF and APG representatives between 31 October 2018 and 15 November 2018. The report was adopted by the APG during its annual meeting which was held in Canberra, Australia between 18–23 August 2019.

A key finding of the report was an assessment that Hong Kong's AML/CTF regime is, overall, compliant and effective. This makes the jurisdiction of Hong Kong one of the leading performers in APAC following the fourth round of FATF and APG evaluations. However, in acknowledging that Hong Kong represents a major finance, trade and transport hub within the APAC region, susceptibility was identified for the jurisdiction as a potential 'transit point' for illicit funds generated in external jurisdictions. In this regard, it was highlighted that corruption and tax evasion are key AML/CTF threats for APAC as a whole.

To address this risk and increase AML/CTF effectiveness in Hong Kong, the report included the following recommended actions:

1. Take steps to more closely review money-laundering threats arising from corruption and tax evasion.
2. Update understandings of cross-border cash smuggling risks.
3. Document and complete an update on the AML/CTF risk assessment and the exemptions applied to stored value facilities.
4. Review vulnerabilities relating to stand-alone financial leasing companies.
5. Undertake a more comprehensive assessment of the money-laundering risks posed by legal persons and trusts.
6. Review and implement appropriate AML/CTF requirements for dealers in precious metals and stones.[8]

In addition to the recent mutual evaluation attendance on Vietnam, the APG has commenced evaluations of Japan and Korea (jointly with the FATF) as well as Tonga.[9]

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

In addition to membership to FATF-APG, Australia and many other APAC countries are signatories to the *United Nations Convention against Transnational and Organised Crime*. Signed on 13 December 2000 and ratified on 27 May 2004,[10] the Convention includes an agreement that each state party:

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

In a conference hosted by Vienna between 15–19 October 2018, the UNTOC adopted the 'Establishment of the Mechanism for the Review of the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto'. The mechanism represents a means to gather information and review the performance of signatories to the United Nations Convention.

Following a preparatory phase, reviews are scheduled to commence in 2020–2021.[11]

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

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

1. giving clear focus to supporting Member States and regional partners in achieving priority crime and drug outcomes in the region; and
2. increasing the responsiveness, efficiency and effectiveness of UNODC's support to the region.[12]

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

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

Commencing on 20 April 2020 and concluding on 27 April 2020, Kyoto, Japan will host the 14th United Nations Congress

on Crime Prevention and Criminal Justice. The agenda for this conference, which represents a gathering of policy-makers, legal practitioners, academics and government agency representatives, includes follow-up to the implementation of the Doha Declaration. The Doha Declaration was adopted at the 13th United Nations Congress on Crime Prevention and Criminal Justice held in Qatar.

The declaration represents the foundation agreement for a global programme to be implemented by UNODC to assist jurisdictions, including APAC jurisdictions, in achieving crime prevention, criminal justice, corruption prevention and upholding the rule of law.[13]

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

In the 2017 joint APG and UNODC research report titled *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime*, it was identified that the illegal wildlife trade is now an entrenched feature of transnational organised crime, with global proceeds estimated in the region of 7–23 billion USD annually.[14]

Despite the significant cash flows and transnational nature of this criminal typology, the outcomes of the research conducted highlighted multiple regulatory and law enforcement vulnerabilities in the region. For example, in many Asia-Pacific jurisdictions, wildlife crime does not constitute a predicate offence to money laundering and a majority of Member States do not presently include Financial Intelligence Unit ('FIUs') in multi-agency anti-wildlife crime taskforces.[15]

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

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

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

The section below focuses primarily on the role of Australian financial intelligence and law enforcement agencies operating within the APAC region. The Australian government anticipates continuing its leadership in promoting global standards for combatting money laundering and expressly provides for increased bilateral cooperation and diplomatic engagement with international law enforcement partners.[16]

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

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

Members include:

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

The express purpose of the PTCN and the PICP is to build policing leadership in the Pacific region and collectively navigate regional policing challenges through discovery, knowledge, influence and partnerships.[17]

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

AUSTRAC has a dual function as both Australia's specialist FIU and the country's anti-money laundering and counter-terrorism regulator. Tasked with identifying emerging threats and existing contraventions within the financial system, AUSTRAC's regulatory and investigative powers are set out under the *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) ('AML/CTF Act') and the *Financial Transactions Reports Act 1988* (Cth).

AUSTRAC's primary role as a law enforcement agency is the receipt and analysis of financial data, which can in turn be disseminated as intelligence to revenue, law enforcement, national security, human services, regulatory and other partner agencies in Australia and overseas.[18]

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

Memorandums of understanding ('MoU') are presently in place between AUSTRAC and 93 other equivalent national FIUs. This includes successful agreements signed with prominent regional partners: China Anti-Money Laundering Monitoring and Analysis Centre ('CAMLMAC') on 2 November 2016;[19] and the United States counterpart, the Financial Crimes Enforcement Network ('FinCEN') on 27 September 2018.[20]

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

1. the foreign government requesting the information has provided requisite undertakings as to the protection of confidential information, controlling the use of the information, and assurances have been provided that the use of the information is only for the communicated purpose;[21] and
2. it is appropriate to release the information in all the circumstances.

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

AUSTRAC provides extensive technical assistance and training programmes throughout the Asia-Pacific region to strengthen the effectiveness of counterpart FIUs. Formal training programmes focused on capability building have been administered in Bangladesh, Cambodia, Indonesia, Nepal, Papua New Guinea, the Philippines and Thailand.[22]

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

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

The AFP has demonstrated an increased strategic shift from domestic law enforcement measures towards increased international engagement. Published in 2017, the *International Engagement: 2020 and Beyond Report* recognises the need to increase collaboration with foreign law enforcement partners to combat 'the growth in criminal and terrorism threats from offshore, the continued global integration of markets and services, and the ongoing disruption of digital technologies'.[23]

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

1. increased strategic engagement with international partners;
2. the conducting of transnational operations which deliver operational effect offshore;
3. information and criminal intelligence sharing; and
4. mutual capability building.[24]

The AFP now has in excess of 300 active personnel posted in over 52 separate locations internationally, including several postings with partners in Asia, South-East Asia and the Pacific catchment.[25]

In order to address offences including money laundering and transnational financial crime, the AFP has in recent times established memorandums of understanding ('MoU') with agencies in APG partner jurisdictions, including the Federal Bureau of Investigation in 2015,[26] the Cambodian National Police in 2016[27] and the Chinese National Commission of Supervision in 2018.[28]

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

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

1. Collecting criminal intelligence from partner agencies and combining it to create a comprehensive national database.
2. Utilising extensive coercive powers under the *Australian Crime Commission Act 2002* (Cth) to obtain information.
3. Acquiring strategic intelligence products to support in decision-making, strategic targeting and policy development.
4. Implementing a national target management framework to guide law enforcement in establishing and sharing organised crime priorities and targets. This is particularly useful for dealing with multi-jurisdictional serious and organised crime investigations.[29]

The ACIC participates in a number of national law enforcement taskforces in both a formal and informal capacity. Contributing unique investigative capabilities, the ACIC provides an 'intelligence-led' response to serious and organised crime.[30]

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

Money laundering is similarly identified as one of the serious organised criminal activities adversely affecting the National interests of Australia and an identified area of operations for Task Force Vestigo. Led by the ACIC, the task force includes Australian Commonwealth, state and territory partners as well as Five Eyes Law Enforcement Group, which comprises law enforcement and intelligence agencies from Australia, Canada, New Zealand, the United Kingdom and the United States.[31]

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

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

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

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

**The Serious Financial Crime Taskforce ('SFCT')**
An Australian multi-agency taskforce which includes:

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

**The Egmond Group**
The Egmond Group is a global network of 156 FIUs committed to collaboration and information exchange. Notable Asia-Pacific members include:

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

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

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

**The Fintel Alliance: Annual Report 2018–2019**
Due to the vast spectrum of expertise held by Fintel Alliance members, highly specialised taskforces can be formed leveraging the skills and experience of the most appropriate members

to tackle a specific threat. Fintel Alliance members leverage the expertise of government, industry, academia and specialised taskforces to disrupt serious crime.

In its 2018–19 Annual Report, AUSTRAC provided some insight into the key achievements of the Fintel Alliance, which include dismantling significant fraud networks and providing vital intelligence, leading to the arrests of nine persons of interest under the Australia's Most Wanted programme. Fintel Alliance members have also closed the accounts of approximately 90 high-risk bank customers over the period.

Six reported operations have been undertaken throughout the period, relating to:

- Scam and money mules.
- Suspect charitable and non-profit organisations ('NPOs').
- Complex fraud and money laundering.
- Credit card fraud and identity theft.

Key collaborations involved the AFP, ACIC, ATO, NSW Police, Australian Charities and Not-for-profits Commission ('ACNC'), IDCARE and Australian Financial Crimes Exchange ('AFCX').

The Annual Report covers Fintel operations including the identification of over 2,500 stolen credit cards and identities, enhanced detection capabilities for scam and money mules, and the identification of the main criminal, money-laundering and terrorism-financing threats currently facing non-profit organisations.[32]

## Money Laundering Typologies: A Diverse Range of Criminal Activities

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

## What Are Some Recent APAC Money Laundering Typologies?

The *APG Yearly Typologies Report 2019* identifies the numerous typologies used to launder proceeds of crime in the Asia-Pacific region. These typologies have been identified following an evaluation of case studies which reflect the present and emerging money-laundering landscape in Hong Kong, Indonesia, Japan, Malaysia, New Zealand, Pakistan, Thailand, Brunei, China, Fiji, Laos, Macao, Singapore and Australia.[33]

1. **Terrorism financing**
   An objective of many types of money-laundering typologies is to ultimately finance acts of terrorism or terrorist organisations. Criminals will seek to obscure money trails in an effort to circumvent targeted financial sanctions imposed against individuals, businesses or countries.
2. **Use of offshore banks, international business companies and offshore trusts**
   As well as being a prevalent typology for taxation-related offences, the use of offshore companies (including shell companies), trusts and financial institutions is a common means to conceal and launder illicit funds.
   'Underground' banks or complex corporate structures may be used, often in jurisdictions subject to less rigorous regulation of such practices.
3. **Cash conversion and currency exchange**
   The use by criminals of travellers' cheques, stored value cards or currency exchange houses to transport money between jurisdictions without direct transfer of funds. The use of cash smugglers is also common in efforts to conceal the movement of currency.
   The proliferation of Bitcoin and other cryptocurrencies has also shown an increase in the illegal use of digital currencies in preference to traditional currencies. This is due to the medium's perceived anonymity and market volatility. Digital currencies also represent the most common currency utilised on the 'dark web', which is again used as a means to maintain anonymity and conceal true ownership. Smart Automatic Teller machines have also been used to make high volumes of illegal cash deposits to third-party accounts while avoiding direct interaction with banking staff.
4. **Use of professional services (lawyers, notaries, accountants, real estate agents)**
   Professionals such as lawyers, financial advisors, real estate agents and accountants are commonly referred to as 'gatekeepers', used to facilitate unlawful transactions, exploit apparent loopholes in AML regulation and abuse positions of trust granted to certain professions. Vulnerable professionals experiencing personal pressures such as debt, addiction or mental health issues may be targeted by criminal organisations.
   The complexity, global scale, and expertise in the provision of services make combatting the activities of professional money launderers a challenging task for law enforcement.
5. **Use of new payment systems or methods**
   Emerging means of transferring funds are often targeted by criminal organisations due to a lag in oversight and regulation. New systems often feature a greater number of money-laundering vulnerabilities when compared to established systems, which have been subject to regulation and reform over an extended period.
   A recent example is the exploitation of Intelligent Deposit Machines utilised by the Commonwealth Bank of Australia, which were used to make in excess of 53,000 suspect transactions which excessed the reporting threshold amount.
6. **Corruption-associated money laundering**
   The use of bribery of public officials and private sector compliance staff to undermine anti-money laundering regulation and reporting measures. This method may also involve the use of corrupt 'gatekeeper' professionals including bankers, lawyers, accountants and brokers who succumb to coercion on the part of criminals or alternatively actively market specialist methods of laundering money.
7. **Structuring**
   Also known as 'smurfing', this method involves a high volume of comparatively small transactions between multiple parties and accounts to avoid detection threshold reporting obligations.
   Difficulty in detection is increased by virtue of the involvement of persons unaware of their participation in such schemes, which involve what would otherwise be a series of legitimate financial transactions.
8. **Use of portable commodities**
   The purchase of high-net-value instruments such as jewellery, diamonds, art works, precious metals, race horses and illicit drugs are used to conceal net worth and property ownership, as well as a means of transporting assets through international points of entry without detection or reporting. There is also a known association between human trafficking offences and money laundering.
   Commodity exchange or barter of such items between parties also can be used to avoid the use of private reporting entities, such as banks. The transnational trade of child pornography, for example, has also been subject to prosecution for money-laundering offences in Australia.[34]
9. **Use of wire transfers**
   Electronic wire transfers between banks and financial

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

10. **Underground banks and alternative remittance services: Hawala, Hundi, etc.**
Such services are identified as underground or unregulated networks of trust-based, intra-jurisdictional transfers used to remit monies. Such methods are commonly used by money launderers parallel to the traditional banking sector.
Alternative remittance providers increase the difficultly by which law enforcement and FIUs can identify individuals or parties controlling funds, as well as obscuring the observable transferor-transferee relationship. Underground banking practices also include illegal card-swiping practices and illegal trading of foreign exchange.
11. **Gambling and gaming activities**
Such methods exploit the high-net-value of assets which are held and pass between parties in the gambling sector. Examples include the use of online gambling or online gaming accounts to conceal the overall value of assets held, the use of winning tickets to conceal crime proceeds and the use of casino chips as currency.
12. **Invoice manipulation and trade-based money laundering**
Both over- and under-invoicing of goods or services can be used in conjunction with import and export activities to obscure movement of funds between international jurisdictions and disguise illegitimate wealth as traditional trade activity. Money laundering that is based on the abuse of trade transactions is achieved by fraudulently misrepresenting the quantity, price or quantity of an import or export.
Such a method is often used in tandem with complex transnational business structures to conceal the identities of individuals involved.
13. **Business investment or 'mingling'**
As one of the key objectives of money-laundering activity, 'mingling' involves the deliberate combining of proceeds of crime with profits from legitimate business enterprises to obscure the source of funds and perpetuate the impression of 'clean' money.
The practice may be combined with false accounting practices to manipulate the observable proportions of profit obtained through legitimate enterprise.
14. **Identity fraud and false identification**
Identity fraud can be used both as a method of concealment to engage in separate money-laundering typologies or as a means of obtaining further illegitimate funds through welfare fraud, superannuation fraud, obtaining fraudulent cash loans or lodgement of false tax returns. Nominees, trusts, family members or third parties may also be used by criminal organisations in an effort to obscure true ownership.[35]

In the ACIC's *Serious Financial Crime in Australia Report 2017*, it was identified that the methodology used to launder proceeds of a crime is also influenced by the area of crime the proceeds originate from. The proceeds of a drug crime, for example, commonly requires large amounts of illegally obtained cash to be deposited into the banking system. Alternatively, financial or 'white-collar' crime often involves the manipulation of accounting practices for money already contained within legitimate banking systems.[36]

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

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

### Strike Force Mactier

Strike Force Mactier represented targeted, collaborative investigations into international money laundering by officers and staff of the NSW Police Force, the NSW Crime Commission, AFP, and the ABF.[37]

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

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

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

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

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

During the course of these search warrants, investigators seized jewellery, vehicles and other property valued in excess of 8.5 million AUD. It is alleged that Chinese nationals had established shell companies in Australia to purchase extensive residential and development property, using funds illegally acquired in China through fraudulent investment.[38]

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

### AUSTRAC – Civil action against Westpac for non-compliance with the AML/CTF Act

On 20 November 2019, AUSTRAC applied to the Federal Court of Australia seeking civil penalty orders against Westpac Banking Corporation, more commonly referred to as Westpac Bank.

It is alleged by AUSTRAC that Westpac Bank has engaged in systematic non-compliance with the AML/CTF Act and has contravened the terms of the legislation on over 23 million separate occasions. The contravening conduct is said to include a failure to:

1. Appropriately assess and monitor money-laundering and terrorism-financing risks associated with transnational transfer of funds to and from Australia.
2. Report over 19.5 million International Funds Transfer Instructions ('IFTIs').

3. Provide separate financial institutions within transfer chains with information relating to the source of funds transferred.
4. Keep records in relation to the origin of internationally acquired funds.
5. Carry out appropriate customer due diligence, particularly in relation to outgoing transactions to the Philippines and South-East Asia with high risk indicators for child exploitation typologies.

The matter has been adjourned for a case management hearing, which is scheduled to occur in late-February or early-March 2020.[39] Each alleged contravention can attract a civil penalty of between 17 million AUD and 21 million AUD, meaning Westpac Bank is currently facing a potential maximum penalty of 391 trillion AUD for their alleged conduct.

## Overview of Laws in Australia

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

### *Criminal Code Act 1995* (Cth)

Money laundering is an offence prohibited at a Federal level under Part 10.2 of the *Criminal Code Act 1995* (Cth) ('Criminal Code'). The provisions cover a wide variety of offending conduct relating to money, or other property, that is used in connection with serious crime. This legislative regime has been described judicially as a '21st century response to antisocial and criminal conduct, commonly with international elements'.[40]

Sections 400.3–400.9 of the Criminal Code include offence provisions which make it an offence to deal with or receive, possess, conceal, dispose, import, export or engage in a banking transaction relating to money or property which represents proceeds or an instrument of crime.[41]

Property will be classified as *proceeds of crime* under the Criminal Code if it is wholly or partly derived or realised (directly or indirectly) by any person from the commission of an indictable offence against a law of the Commonwealth, a State, a Territory or a foreign country.[42]

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

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

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

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

By way of example, if the prosecution can establish beyond reasonable doubt that an accused person deals with money or property that the person believes to be proceeds of a crime (or intends for the property to become an instrument of crime) and the property is valued at 1 million AUD or more, the person is liable to a maximum term of imprisonment of 25 years and or a fine of up to 315,000 AUD.[43]

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

### *Proceeds of Crime Act 2002* (Cth)

As of 1 January 2003, the AFP and the CDPP have been empowered under POCA to seek restraining, forfeiture or freezing orders in relation to property suspected of being connected with a criminal offence.

Typically, assets including actual, real and interests in property become subject to an order if it is established that the property is suspected on reasonable grounds to be the proceeds of an indictable offence, a foreign indictable offence or was previously used in connection with the commission of an offence.[44]

A Court must also make an order that property subject to the application be forfeited to the Commonwealth if a person has been convicted of one or more indictable offences, and the court is satisfied that the property is proceeds or an instrument of one or more of the offences.[45]

It is an express object of POCA to give effect to Australia's obligations under the Council of Europe *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*, and other international agreements relating to proceeds of crime.[46]

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

The conduct of financial institutions in Australia is regulated under the AML/CTF Act. The AML/CTF Act sets requirements for reporting entities including institutions within the financial sector, gambling sector and businesses involved in the trade of bullion.[47]

Obligations are imposed on reporting entities, including a requirement to:

1. enrol and register businesses conducting relevant business;[48]
2. conduct due diligence on all customers including confirmation of identity;[49]
3. retain transaction records for a period of seven years;[50]
4. develop and implement programmes for the detection of money-laundering activity;[51] and
5. report suspicious matters to AUSTRAC.[52]

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

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

Some contraventions under the AML/CTF Act do attract criminal sanctions. It is a criminal offence to provide a designated service under a false name[53] or conduct transactions with the intention of avoiding reporting requirements.[54] Further 'tipping off' offence provisions prohibit contact or communication with persons, other than AUSTRAC personnel, following a referral of suspicious activity. For example, it is a criminal offence under such a provision for a reporting entity, such as a

bank, to notify AUSTRAC of suspicious activity on the part of a customer while simultaneously notifying the relevant customer that their conduct has been reported to AUSTRAC.

The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017* was passed by both houses of Parliament on 7 December 2017 and commenced on 3 April 2018. This amending legislation expanded AUSTRAC's powers under the AML/CTF Act to monitor digital currency markets. As with existing reporting entities within the finance sector, digital currency exchange providers are now required to register under the AML/CTF Act and comply with the obligations set out under the Act.[55]

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

Australia's legislative amendments follow comparable recent regulatory action on the part of the Hong Kong Regulatory Authority, Bank of Negara Malaysia and the Monetary Authority of Singapore.[56] In these jurisdictions, the amendments bring cryptocurrencies and providers of digital currency predominantly in line with traditional financial and property exchange markets, for the purpose of anti-money laundering regulation.

## Conclusion

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

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

## Endnotes


1. Asia/Pacific Group, *Strategic Plan 2016–2020*, 2016, Sydney, p. 11.
2. Asia/Pacific Group, http://www.apgml.org/news/details.aspx?pcPage=1&n=1143, accessed 9 January 2020.
3. Department of Home Affairs, https://minister.homeaffairs.gov.au/peterdutton/Pages/Address-to-the-No-Money-for-Terror-Conference,-Melbourne.aspx, accessed 9 January 2020.
4. Asia/Pacific Group, http://www.apgml.org/mutual-evaluations/page.aspx?p=a901712a-54e4-4b3b-a146-046aefca6534, accessed 12 March 2019.
5. Asia/Pacific Group, http://www.apgml.org/news/details.aspx?n=2155, accessed 31 December 2019.
6. Asia/Pacific Group, http://www.apgml.org/mutual-evaluations/page.aspx?p=c12cf2af-4e56-472c-9201-90d0baf-9ceda, accessed 31 December 2019.
7. Asia/Pacific Group, *Strategic Plan 2016–2020*, 2016, Sydney, p. 8.
8. FATF & Asia/Pacific Group, *Mutual Evaluation Report of Hong Kong, China*, 2019.
9. Asia/Pacific Group, *Annual Business Report 2018-2019*, 2019, Sydney, p. 8.
10. *United Nations Convention on Transnational Organised Crime*, GA Res 55/25, 2000.
11. United Nations, *Establishment of the Mechanism for the Review of the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto*, Res 9/1, 2018.
12. United Nations, https://www.unodc.org/southeastasiaandpacific/en/what-we-do/index.html, accessed 9 January 2020.
13. United Nations, https://www.unodc.org/congress/en/about.html, accessed 15 January 2020.
14. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime*, 2017, Sydney, p. 5.
15. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime, 2017*, Sydney, p. 6.
16. Australian Government, *2017 Foreign Policy Whitepaper*, 2017, Canberra, p. 73.
17. Pacific Islands Chiefs of Police, https://picp.co.nz/about-pacific-islands-chiefs-of-police-picp/vision-purpose-strategy/, accessed 11 March 2019.
18. Miralis, D & Gibson, P, 'Australia: An increasingly global approach', *Global Investigations Review*, 17 September 2019, p. 4.
19. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/media/media-releases/austrac-signs-historic-mou-china, accessed 7 March 2019.
20. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/media/media-releases/australia-strengthens-international-partnerships-fight-against-financial-crime, accessed 7 March 2019.
21. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), s. 132(1)(a).
22. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/about-us/international-engagement/international-assistance-and-training, accessed 7 March 2019.
23. Australian Federal Police, *International Engagement: 2020 and Beyond Report*, 2017, Canberra, p. 4.
24. Australian Federal Police, *International Engagement: 2020 and Beyond Report*, 2017, Canberra, p. 4.
25. Miralis, D & Gibson, P, 'Australia: An increasingly global approach', *Global Investigations Review*, 17 September 2019, p. 4.
26. SBS News, https://www.sbs.com.au/news/afp-fbi-poolresources-against-crime, accessed 7 March 2019.
27. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/afp-and-cambodian-authorities-working-closely-combat-drugs-and, accessed 7 March 2019.
28. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/australia-re-signs-landmark-deal-china, accessed 7 March 2019.
29. Nyman Gibson Miralis, https://ngm.com.au/money-laundering-lawyers/money-laundering-australian-crime-commission-investigations/, accessed 7 March 2019.
30. Australian Criminal Intelligence Commission, https://www.acic.gov.au/about-crime/task-forces, accessed 7 March 2019.
31. Australian Criminal Intelligence Commission, https://www.acic.gov.au/about-crime/task-forces/vestigo-task-force, accessed 7 March 2019.
32. Australian Transaction Reports and Analysis Centre, *Fintel Alliance: Annual Report 2018-2019*, 2019, Sydney, pp. 35–47.
33. Asia/Pacific Group, *APG Yearly Typologies Report 2019: Modern Trends of Money Laundering and Terrorism Financing*, 2019, Canberra, Australia.
34. *Dennison v R* [2011] NSWCCA 114.

35. Asia/Pacific Group, *APG Yearly Typologies Report 2019: Modern Trends of Money Laundering and Terrorism Financing*, 2019, Canberra, Australia.
36. Australian Criminal Intelligence Commission, *Serious Financial Crime in Australia Report 2017*, Canberra, p. 12. Asia/Pacific Group & United Nations Office on Drugs and Crime, *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime, 2017*, Sydney, p. 5.
37. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/five-charged-and-180000-seized-over-alleged-international-money-laundering, accessed 7 March 2019.
38. Australian Federal Police, https://www.afp.gov.au/news-media/media-releases/afp-operation-targets-chinese-nationals-allegedly-laundering-proceeds, accessed 7 March 2019.
39. Australian Transaction Reports and Analysis Centre, https://www.austrac.gov.au/about-us/media-release/civil-penalty-orders-against-westpac, accessed 9 January 2020.
40. *R (Cth) v Milne (No 1)* [2010] NSWSC 932 at [164].
41. *Commonwealth Criminal Code Act 1995* (Cth), s. 400.2.
42. *Commonwealth Criminal Code Act 1995* (Cth), s. 400.1.
43. *Commonwealth Criminal Code Act 1995* (Cth), s. 400.3.
44. See *Proceeds of Crime Act 2002* (Cth) ss. 15B; 329.
45. *Proceeds of Crime Act 2002* (Cth) s. 48.
46. *Proceeds of Crime Act 2002* (Cth) s. 5.
47. Australian Transaction Reports and Analysis Centre, http://www.austrac.gov.au/businesses/legislation/amlctf-act, accessed 7 March 2019.
48. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 7.
49. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 28.
50. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 107.
51. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 81.
52. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 41.
53. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth) s. 139.
54. *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), s. 142.
55. *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017* (Cth), Part 2 s. 4.
56. Deloitte, *Asia Pacific Regulatory Update*, 2018, Sydney, p. 1.

## Acknowledgments

The authors would like to thank Jasmina Ceic and Damien Mahon for their invaluable contribution to the writing of this chapter.

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

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

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

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

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

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

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

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

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

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

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

**www.ngm.com.au**

NYMAN GIBSON MIRALIS
Defence Lawyers and Advisors est. 1966

# Argentina


Maximiliano D'Auro


Rodrigo Allende

Beccar Varela



## 1 The Crime of Money Laundering and Criminal Enforcement

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

Argentina is currently undergoing a process to substitute the National Criminal Procedural Code ("NCPC") for the recently enacted Federal Criminal Procedural Code ("FCPC"). While according to the NCPC, the legal authority to prosecute money laundering at the national level is the Federal Judge – that is also entitled to delegate the investigation to the Federal Prosecutor – the new FCPC establishes that the Federal Prosecutor must carry out all prosecutions. Currently the FCPC has been implemented in just a few jurisdictions (those being the provinces of Salta, Jujuy and Mendoza and the City of Rosario, Santa Fe). The rest of the jurisdictions still operate under the rules of the NCPC.

There is also a special prosecution unit for economic crimes and money laundering that is intended to assist prosecutors when dealing with these kinds of cases.

Finally, Argentina's criminal system also allows for claimants ("*querellantes*") to intervene and be part of the accusation. The Financial Information Unit ("UIF"), an agency created to lead the Administration's AML efforts, is entitled to intervene as a claimant in money laundering-related cases.

### 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 303 of the National Criminal Code ("NCC") establishes penalties imposed on whoever introduces (or tries to introduce) in the market goods or funds that are the proceeds of an illicit activity, with the possibility that those goods (or other subsequent goods) acquire the appearance of being of legal origin. In this scenario, apart from proving the introduction or intent of introducing proceeds of criminal activity, the prosecution must prove that in fact those goods are related to a criminal offence. The NCC does not establish the extent to which the relationship between the goods or funds and the predicate offence has to be proven. Courts, on the other hand, have understood that the existence of a predicate offence can be proved by any means and with a lower evidence standard than that of the money laundering crime – without having the need to fully identify neither the perpetrator nor the entire causal link between that activity and the goods or funds objects of the money laundering offence.

The NCC does not limit the offences that can be included as precedent crimes, so it is understood that the goods that proceed from the commission of any criminal offence can be considered the predicate of a money laundering offence, tax evasion included.

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

Argentina's NCC only applies in Argentina. However, the NCC does specifically establish that money laundering is punishable when the predicate illicit activity was committed in a foreign jurisdiction.

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

As noted in question 1.1, the Federal Courts and Federal Prosecution are the main government authorities responsible for investigating and prosecuting money laundering. With certain limitations, UIF and the Central Bank ("BCRA") are qualified to conduct investigations and to file reports to the Federal Courts and Prosecution.

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

The NCC establishes corporate criminal liability for money laundering offences. In particular, Section 304 NCC establishes that corporations can be held liable if the offence is committed in the name, benefit or with the intervention of the corporation.

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

The maximum penalty applicable to individuals convicted of money laundering crimes is 10 years imprisonment and a fine equal to 10 times the amount of the illegal transaction made or intended to be made. If the offender is dedicated to the money laundering activity, is a member of a criminal group, a public official or a member of a regulated activity, the imprisonment penalty limit is raised up to 13 years.

Corporations may also be sanctioned with fines equal to 10 times the amount of the value of the transaction made or intended

to be made and total suspensions of their activities for up to 10 years. Legal entities created with the sole intention of committing criminal offences may have their legal existence terminated.

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

The statute of limitations for money laundering crimes is 10 years.

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

Enforcement of these crimes was traditionally understood to be at national (federal) level. However, in recent years, different jurisdictions have challenged this position and some provincial courts have claimed competence over money laundering crimes. Most notably, the Supreme Court of the Province of Santa Fe held on February 2020 that provincial authorities are competent to enforce money laundering offences. This subject must still be decided by the National Supreme Court in order to produce a definitive answer.

There are no parallel provincial 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?**

Only the Courts can forfeit/confiscate property. Section 23 NCC establishes that the Court in its criminal sentence can decide to confiscate any property that was used to commit a criminal offence and all goods and funds that proceed from that crime. The rule is that all property can be subject to confiscation.

"Embargos", a kind of temporary confiscation, may also be used as a precautionary measure in order to protect property that may be subject to confiscation in the final sentence.

In cases where there is sound suspicion of terrorist financing or terrorist financing-related activity, UIF is entitled to order the freezing of the suspected assets for up to six months. This decision can be challenged in Criminal Courts.

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

Currently, there has been no conviction of banks or other regulated financial institution for money laundering offences.

In the hypothetical case in which a financial institution is convicted of a money laundering offence, the BCRA may consider this sufficient reason to forfeit that bank's licence.

**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?**

Given the severity of the potential sentences for money laundering crimes, there are no alternatives to judicial processes to resolve criminal actions.

The exception would be that of "minor cases" of money laundering (in which the amount of the transaction does not exceed AR$300,000), with a maximum sentence of three years. In this case, the defendant and prosecution can agree on a plea bargain that later must be homologated by a Court.

## 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.**

Law nr. 25.246 regulates anti-money laundering ("AML") in Argentina, created UIF and tasked this entity with coordinating the Administration's AML efforts and policies. Even though UIF is the main administrative authority responsible for imposing AML measures, the BCRA and the National Securities Commission ("CNV") also have limited authority to impose AML requirements within their scope of competence.

UIF has adopted the Financial Action Task Force ("FATF") 2012 Recommendations. As a consequence, it has been enforcing a set of requirements over regulated entities with a risk-based approach and aims to prevent money laundering and terrorist financing. These requirements include: AML training for personnel; costumer due diligence and record keeping; internal controls; reporting of suspicious activity; transparency on legal ownership; and the identification of final beneficiaries, among others.

In particular, the AML requirements for financial institutions are regulated in UIF Resolution nr. 30/2017.

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

There are no AML requirements imposed by self-regulatory organisations.

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

No, organisations and professional associations are not responsible for anti-money laundering compliance and enforcement.

**2.4 Are there requirements only at national level?**

There is AML regulation only at national level. Provinces do not have the competence to regulate in this regard.

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

UIF is the government competent authority responsible for examining compliance and enforcement of AML requirements. Other than what is stated in its regulation, the criteria for examination can be casuistically inferred from the considerations made as motivation for each of the sanctions imposed. These sanctions are publicly available on the Agency's web page.

**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?**

Law nr. 25.246 tasks UIF with analysing financial information in order to help prevent and detect money laundering and terrorist financing-related criminality. In order to do this, UIF receives from all of the "Obliged Subjects" (the persons and entities subject to AML regulations) suspicious activity reports and periodic relevant transactions reports. This information may lead to the implementation of new preventive measures and the reporting of potential criminal activity to the competent authorities.

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

The statute of limitation to bring enforcement actions in the case of criminal offences is 10 years. Administrative enforcement from UIF to entities subject to AML requirements is 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?**

The maximum penalty for failure to comply with the requirements is a fine of up to 10 times the value of the goods or the transaction the failure refers to. If the value of the goods cannot be determined, the fine has a cap of AR$100,000.

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

UIF is only entitled to impose fines. As described in question 1.6, Courts may impose more serious penalties in the case of money laundering crimes.

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

All of the penalties are administrative fines. The regulation does not consider any other kind of sanction for entities subject to AML requirements or its directors, officers or employees.

**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 conducted by UIF, which is also the authority that imposes the sanction. While the process is confidential, the decision to sanction is public and is usually uploaded to UIF's web page. Sanctions imposed by UIF can be challenged in judicial proceedings at the Court of Appeals of Federal Administrative matters. Financial institutions sanctioned by UIF have challenged penalty assessments on several occasions.

## 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.**

Law nr. 25.246 establishes in its Section 20 the following 23 categories of businesses and professionals that are subject to AML requirements and are referred to as "Obliged Subjects": i) financial entities; ii) foreign exchange entities; iii) companies/persons whose activity is gambling (casinos, lotteries, etc.); iv) stock market agents and all persons authorised by CNV to operate in the securities market and those operating in managing investment funds and related activities; v) person authorised by the CNV to operate in the futures and equity market; vi) public commercial registries; vii) persons and entities that operate in the fine arts, antiques, jewellery and luxury goods markets; viii) insurance companies; ix) credit card and travellers' cheques companies; x) treasury and cash transport companies; xi) postal service companies; xii) public notaries; xiii) capitalisation entities; xiv) customs brokers; xv) the BCRA, the Federal Agency of Public Revenues ("AFIP"), the Superintendence of Insurance, the National Securities Commission ("CNV"), the General Inspection of Justice ("IGJ"), the National Institute for Associations and Social Economy, and the Antitrust Court; xvi) insurance producers, consultants, agents and brokers; xvii) licensed professionals whose activities are regulated by professional councils or associations of economic sciences (certified public accountants and auditors); xviii) legal entities that regularly receive donations; xix) licensed real estate agents or brokers and real estate brokerage corporations; xx) mutual and co-operative associations; xxi) natural persons or legal entities whose usual activity is the sale or purchase of cars, trucks, motorcycles, buses, agricultural machinery, road machinery, boats, yachts, and airplanes; xxii) 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 xxiii) legal entities that organise and regulate professional sports.

The categories are broad and the final specification of the natural and legal entities that fall within the categories of Section 20 are defined in UIF's specific regulation. Businesses engaged in offering new payment technologies or alternative currencies may or may not fall within category "i) financial entities", depending on the kind of service offered. According to UIF Resolution nr. 30/17, the term financial entity must be understood as those under the BCRA's oversight and regulated under laws nr. 21.526 or nr. 18.924. As an example, a digital wallet is not generally considered a financial entity, so it would fall outside the AML requirements and not be considered an "Obliged Subject". On the other hand, a company that takes deposits and grants loans will be generally considered a financial entity and, thus, is subject to AML requirements.

Within gatekeepers, the regulation focuses only on public notaries and certain specific economic sciences professionals, those with responsibilities auditing corporate balance sheets or with the functions of corporate controller.

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

In Argentina, cryptocurrency operations are considered to entail

a high ML risk. As such, UIF has mandated that all Obliged Subjects must report monthly all of the cryptocurrencies transactions in which they take part and apply to them rigorous AML measures.

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

All of the Obliged Subjects are required to maintain AML compliance programmes. Until 2017, UIF had a formal approach to the subject and required Obliged Subjects to comply with a series of requisites: 1) having an AML policy; 2) designating a compliance officer; 3) KYC policy; 4) training employees in AML; 5) reporting of suspicious transactions; and 6) periodic reporting of relevant transactions. Since 2017, and after adopting FATF's 2012 Recommendations, UIF has issued a new regulation that requires a risk-based approach to AML. In this sense, now Obliged Subjects are required to conduct an AML risk assessment and design their policies and preventive measures based on the findings. Currently, this new approach is only mandatory for financial institutions (UIF Resolution nr. 30/17), stock market agents and all persons authorised by the CNV to operate in the securities market (UIF Resolution nr. 21/18), insurance companies (UIF Resolution nr. 18/19) and credit card and travellers' cheque companies (UIF Resolution nr. 76/19), though it should be gradually implemented in the rest of the Obliged Subjects.

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

All of the Obliged Subjects need to keep records of their costumers with a certain grade of detail. Mainly, they are required to be able to identify the costumer and create a transactional report for each costumer. They are also required to keep these records for at least 10 years.

Financial institutions must make three types of reports: i) Cash Transactions Report: for every transaction over AR$280,000 (or equivalent in foreign currency), that must contain the identity of the persons or entities making and receiving the transaction, type of transaction, and date, amount and currency of the transaction; ii) Cross-Border Transactions Report: for all of the transactions made to an account abroad, that must contain the type of transaction, the date, amount and currency of the transaction, the country of origin/destiny of the transaction, the identity of the financial entity of origin/destiny, the identity of the holder of the account involved, information of the people related to the account receiving the transaction and those of the account sending the transaction; and iii) Annual Systematic Report: general information of the financial entity with a detail on the number and type of costumers it has.

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

As explained in questions 3.4 and 3.2, other than large cash transactions, all cross-border transactions and all transactions involving cryptocurrencies must be also reported.

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

As mentioned in question 3.4, financial entities must report all international/cross-border transactions.

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

Financial institutions must first identify the customer and require certain documents and information as means of proof of the identity and other relevant information (PEP, authorities and final beneficiaries' affidavits are mandatory). From the information provided, the financial institution must classify the customer into one of at least three risk categories: Low; Mid; and High. Each risk category corresponds with one type of KYC due diligence procedure.

Low-risk customers are screened through a simplified due diligence procedure where the information provided is contrasted against publicly available information and the person/entity is checked against UIF's database on persons and entities linked to terrorist organisations. This category is reserved for people who only own a sole bank account, the balance of which is under AR$421,875 and with cash transactions under AR$67,500. Persons that fall under the PEP category cannot be subject to the simplified due diligence procedure.

Medium-risk customers that do not qualify for simplified due diligence are required to also provide information referring to their economic activity and an affidavit on the licit origin of the funds.

High-risk costumers are screened through an enhanced due diligence procedure in which they are asked for documentation that proves their identity, that of the authorities of the entity, documents that prove the licit origin of the funds and any other additional information the financial entity may find relevant according to the risk profile of the customer.

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

Financial institution accounts for foreign shell banks are prohibited. BCRA rules (Communication A 6709) expressly prohibit opening accounts for "Shell Banks" ("*banco pantalla*") and any financial entity whose supervision authority in its country of origin has not adhered to the Core Principles of Banking Supervision of the Basel Committee on Banking Supervision.

**3.9 What is the criteria for reporting suspicious activity?**

Financial entities must create a transactional profile of each of its customers, consisting of the information collected in the onboarding process, the due diligence procedure and the log of historic transactions. The regulation states that each financial entity must also have procedures to provide alerts when activity is "unusual" based on the costumer profile, his determined risk category and the potential abnormality of the transaction.

Once an activity is labelled as unusual, the financial entity must analyse it in depth and conclude if it can be considered a suspicious activity or not. In order to do so, it can ask for further information and documentation to the customer. At this stage and all through the analysis and potential report, all the elements of the investigation must be kept strictly confidential.

If the entity concludes that the activity is suspicious, it must report it within 15 days after the determination and never more that 150 days after the activity was conducted or attempted. Failing to comply with these terms can result in administrative sanctions.

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

Government maintains current and adequate information about ownership management and ownership, including final beneficiaries. The public registries of each jurisdiction collect this information as part of the mandatory requirements. Financial institutions usually do not deal directly with the registries but require customers, in their onboarding procedures, to provide certifications that contain beneficial ownership information. Depending on the financial institution's AML programme, this information is updated periodically with new requirements.

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

Payment orders funds transfers must be completed with accurate information about the originators and beneficiaries. If there are other financial institutions involved in the transaction, this information should be also available to them in the payment instructions.

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

No. Bearer shares are not permitted in Argentina.

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

As stated previously, there are a significant number of non-financial institution businesses that have specific AML requirements.

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

Within persons engaged in international trade, Argentina's regulation only addresses custom brokers who are "Obliged Subjects" under Section 20 Law nr. 25.246, and specific AML requirements apply to them all.

## 4 General

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

Financial institutions should specially consider the BCRA's regulation concerning AML matters (Communication "A" 6709) and the National Securities Commission ("CNV") regulation, specifically Title XI of the "National Securities Commission Regulations".

**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 been progressing in its compliance with FATF's recommendations but it is still far from total compliance. Even though in the last couple of years there have been important improvements in the AML regulation system, there are serious deficits in the implementation and enforcement of AML measures and sanctions.

Currently, Argentina still lacks a proper money laundering and terrorist financing risk assessment. This deficit means that it has not been able to properly implement a nationwide risk-based approach to the matter, and resources are still being allocated without a clear notion of their efficiency.

UIF's resources also seem very limited in comparison to the task it is responsible for. At the moment, it has not even been able to enact the regulatory transition to a risk-based approach to more than a few of the Obliged Subjects.

Lastly, within the judicial system, enforcement of money laundering sanctions has also been very poor. Procedures for this kind of criminality are extremely long and condemnatory sentences happen rarely, at a rate of no more than one per year.

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

Argentina's last evaluation by an outside organisation was made by FATF in 2010. FATF found that Argentina had failed to adopt and implement most of the recommendations of the previous evaluation and, as a consequence, the plenary decided to put Argentina in the enhanced follow-up procedure. It was not until 2014 that this decision was lifted after the country showed significant progress in its AML compliance and efforts to comply with a significant portion of the recommendations.

Even though Argentina's situation has improved since 2014, the country is still non-compliant or partially non-compliant with a number of FATF's recommendations. The next mutual evaluation will be carried out in 2021.

The 2010 FATF Mutual Evaluation Report can be found here: https://www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationofargentina.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?**

All of Argentina's norms can be found in the Ministry of Economics' free access database "Infoleg": http://www.infoleg.gov.ar. UIF's regulation is also uploaded on the agency's web page: http://www.uif.gov.ar. All of this information is only available in Spanish.

**Maximiliano D'Auro** is a Partner at Beccar Varela where he heads the Anti-Corruption and Compliance Department.
He has broad experience in banking and financial law, advising both foreign and local financial institutions and providing legal advice in all aspects of anti-corruption laws, regulations and compliance.
Maximiliano obtained his Law degree from Universidad Nacional de Mar del Plata (1997) and his Master of Laws (LL.M.) from the London School of Economics (2000). He worked as foreign associate at Gómez-Acebo & Pombo (Barcelona, Spain, 2003).
He is a member of the International Bar Association (IBA) and he is the Latin American Representative of the IBA's Anti-Corruption Committee, as well as the Argentine contributor for the IBA's Anti-Money Laundering Forum. He has participated as a speaker in many conferences and written articles on anti-corruption, commercial fraud, anti-money laundering, asset tracing and recovery. Maximiliano was invited by the OECD to participate, as a private practitioner, in the evaluation of Argentina in the OECD Convention on Foreign Bribery (Buenos Aires, 2014).
He has been recognised by *Chambers Latin America*, *Chambers Global*, *The Legal 500*, *Who's Who Legal*, *Latin Lawyer 250*, *LACCA Approved*, *LACCA Thought Leaders*, *IFLR1000* and *GIR 100*.

**Beccar Varela**
Edificio República, Tucumán 1, 3rd Floor
C1049AAA Buenos Aires
Argentina

Tel: +54 11 4379 6800 / 4700
Email: mdauro@beccarvarela.com
URL: www.beccarvarela.com

**Rodrigo Allende** is a Senior Associate at Beccar Varela and a member of the Anti-Corruption and Compliance Department. He has broad experience in criminal law, anti-corruption and compliance in the public and private sectors.
Rodrigo obtained his Law degree from the Universidad de Buenos Aires (2010), his specialisation in Criminal Law from the Universidad Torcuato Di Tella (2014) and his Master's degree in Criminal Justice from the Universidad Carlos III de Madrid (2017).

**Beccar Varela**
Edificio República, Tucumán 1, 3rd Floor
C1049AAA Buenos Aires
Argentina

Tel: +54 11 4379 6800 / 4700
Email: rallende@beccarvarela.com
URL: www.beccarvarela.com

Founded in 1897, Beccar Varela is a leading full-service law firm in Argentina, placing utmost priority on client service. With our main office in the heart of Buenos Aires and a branch in northern Buenos Aires, the firm has a widely acknowledged practice, advising clients in Argentina and abroad for over 120 years.
Our team consists of over 160 lawyers specialising in different areas of law, many of whom have studied or worked in the world's business capitals. They are supported by motivated paralegals and interns, and by talented and creative administrative staff. A commitment to innovation and an integrated corporate sustainability programme underpins our work.
Accompanying the growing needs of our clients to address local and cross-border compliance and anti-corruption matters, locally and internationally, our firm was a pioneer offering compliance services among the full-service law firms in Argentina. We were also the first full-service firm to develop a white-collar & corporate crime department, making our compliance department the most comprehensive in the market with vast experience in internal investigations and criminal proceedings.
We offer guidance on business integrity and ethics; anti-money laundering and the financing of terrorism; risk analysis and design, development and implementation of anti-corruption and anti-fraud codes of conduct, policies and procedures; internal investigations and asset tracing and recovery. We also advise on the impact of integrity programmes in determining criminal liability for a company, its shareholders and directors, particularly under the new Corporate Criminal Liability Law.
We have worked with the best law firms in the USA, Brazil and other countries in complex cross-border investigations, both internally and with the intervention of foreign authorities (DoJ, SEC).
We are the first and only leading law firm in Argentina to join the United Nations Global Compact, and we are members of the B20 Task Force on Integrity and Compliance.

**www.beccarvarela.com**

BECCAR VARELA

# Australia


Kate Jackson-Maynes

Amelia Jamieson

King & Wood Mallesons


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the 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.

In a discussion paper on corporate criminal responsibility released in November 2019, the Australian Law Reform Commission (ALRC) recommended legislative reform to enable senior personnel of a corporation to be held personally liable for the conduct of a corporation where they are in a position to influence the relevant conduct and failed to take reasonable measures to prevent the corporation's conduct. The discussion paper also considers a due diligence defence for corporate criminal liability. The ALRC intends to publish its final report on 30 April 2020.

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

The maximum penalties for money laundering offences vary depending on the value of the money or property that has been dealt with and the degree of knowledge of the offender. For individuals, the maximum penalty under the Criminal Code is 25 years of imprisonment and a fine of A$315,000 (i.e. 1,500 penalty units) for an offence of dealing with the proceeds of crime which have a value of A$1,000,000 or more, where the person believes the money or property to be the proceeds of crime. For bodies corporate, the maximum penalty for the same offence is a fine of A$1,575,000 (see *Crimes Act 1914* section 4B). The value of a penalty unit under Commonwealth law is due for indexation on 1 July 2020.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

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

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

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

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

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

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

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

**2.4 Are there requirements only at national level?**

Yes, there are requirements only at national level.

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

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

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

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

AUSTRAC has published an information paper on its approach to regulation on its website: https://www.austrac.gov.au/about-us/corporate-information-and-governance/policies-plans-and-commitments/austrac-policies/austracs-approach-regulation.

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

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

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

The maximum penalty for breach of a civil penalty provision under the AML/CTF Act is A$21 million per breach for a corporation or A$4.2 million for an individual. Most of the key obligations under the AML/CTF Act are civil penalty provisions.

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

Civil and criminal actions can also be resolved through the imposition of enforceable undertakings and infringement notices.

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

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

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

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

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

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

The Banking Executive Accountability Regime (BEAR) contained within Part IIAA of the *Banking Act 1959* came into force in July 2018 for Australia's four major banks and in July 2019 for all other banks. The BEAR establishes two sets of accountability obligations: firstly, on banks; and secondly, on their nominated directors and executives (known as 'accountable persons'). The BEAR allows the Australian Prudential Regulation Authority (APRA) to disqualify banking directors or executives from being an 'accountable person' if they have not acted with honesty and integrity, and with due skill, care and diligence. This obligation may be breached if the entity does not have in place appropriate processes, procedures and controls. The BEAR also places an obligation on banks to adjust an accountable person's variable remuneration as a result of a breach of accountability obligations.

A breach of the AML/CTF Act may not necessarily involve a breach of the BEAR but if the entity failed to have in place appropriate processes, procedures and controls in relation to meeting its AML/CTF obligations, then this may result in a breach of BEAR.

In January 2020 the Australian government proposed that this regime be extended to general insurers and superannuation licensees and commissioned a consultation paper to be authored by Federal Treasury, with a view to introducing legislation by the end of 2020.

**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 3.9 below). It is also a criminal offence to provide, possess or make a false document, operate a designated service under a false name, or conduct cash transactions with the aim of avoiding reporting requirements. Operating an unregistered remittance business or unregistered digital currency exchange business will also attract criminal sanctions.

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

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

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

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

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

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

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

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

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

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

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

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

Yes. The AML/CTF Program generally must be composed of a Part A and a Part B and specifically address matters prescribed by the AML/CTF Act and AML/CTF Rules. These matters generally align with the obligations under the AML/CTF Act outlined in the response to question 2.1 above. The primary purpose of Part A is to identify, mitigate and manage the risk the RE may reasonably face that the provision by the RE of designated services at or through a permanent establishment of the RE in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering or terrorism financing. The sole or primary purpose of Part B is to set out the applicable customer identification procedures for the purposes of the application of the AML/CTF Act to customers of the RE.

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

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

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

Yes. REs must report suspicious matters to AUSTRAC (see the response to question 3.9 below). There is also an obligation on persons who send international funds transfer instructions (IFTIs) out of Australia, or who receive IFTIs transmitted into Australia, to report those IFTIs to AUSTRAC. 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.

In February 2020 a Senate committee handed down a report recommending that the Senate pass the Currency (Restrictions on the Use of Cash) Bill 2019 (the Bill) which, if enacted, will ban making or accepting cash payments of A$10,000 or more. The Bill was passed by the House of Representatives in October 2019. The Bill creates strict liability offences that apply if an individual or entity makes or accepts a cash payment (or series of payments) and more serious offences that apply where the individual or entity intends or is reckless about making or accepting such a payment (or series of payments).

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

See the response to question 3.5 above.

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

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

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

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

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

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

Yes. A financial institution must not enter into a banking relationship with a shell bank or a banking institution that has a

banking relationship with a shell bank. If a bank subsequently finds out that it is in a shell bank arrangement, it must terminate the relationship within 20 business days. The definition of shell bank in the AML/CTF Act covers financial institutions and affiliates which have no physical presence in the country they are incorporated in.

### 3.9 What is the criteria for reporting suspicious activity?

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

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

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

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

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

Suspicious matter reporting does not constitute a legal safe harbour or defence to prosecution of the RE for a criminal offence (including money laundering offences), although if the RE gives AUSTRAC information in a suspicious matter report, the RE is taken not to have been in possession of that information at any time for the purposes of the money laundering offences in the Criminal Code.

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

The Australian Securities and Investments Commission (ASIC) maintains information about each Australian company's directors, shareholders and ultimate holding company. ASIC does not maintain information about the natural persons who are the entities' ultimate beneficial owners. This means that the register may not assist in compliance with beneficial ownership requirements.

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

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

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

Beneficiary institutions may give ordering institutions a written notice requesting that the ordering institution provide certain information about the payer. Ordering institutions must comply with such a notice within three business days after the day on which the request was given (or within 10 business days if the request was given more than six months after the transfer instruction was originally accepted by the ordering institution).

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

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

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

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

Yes. See the response to question 3.1 above. There is also a proposal to extend the AML/CTF Act to other areas including lawyers, accountants and real estate agents (although this proposal has been on foot since 2006).

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

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

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

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

## 4 General

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

A statutory review of the AML/CTF Act was undertaken by the Commonwealth Attorney-General's Department in 2013 to 2016 which resulted in 84 recommendations in relation to Australia's AML/CTF regime. The government is in the process of implementing the recommendations in phases. The first phase, which has been implemented, addresses the regulation of digital currency exchange providers, AUSTRAC's power to issue infringement notices and some deregulatory measures. As at March 2020, the next phase is before Parliament for debate and includes changes to customer identification requirements (including expanding the circumstances where REs can rely on the KYC carried out on customers by third parties), exemptions to the prohibition on tipping off and the use and disclosure of financial intelligence (among other changes).

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

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

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

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

Yes. FATF evaluated Australia's AML/CTF regime in 2014 to 2015, releasing its report in April 2015. The report is available on FATF's website http://www.fatf-gafi.org/documents/documents/mer-australia-2015.html. In November 2018, FATF published a follow-up report noting a small improvement in Australia's compliance but without any significant improvement in the issues listed in question 4.2 above: http://www.fatf-gafi.org/media/fatf/documents/reports/fur/FUR-Australia-2018.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 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** is a Partner in the Banking and Finance team of King & Wood Mallesons.
Kate has 20 years' experience advising on the full range of financial services regulation including anti-money laundering and counter-terrorism financing, sanctions, privacy, responsible lending, banking and financial services regulation and payments laws and the ground-breaking areas of blockchain and regtech.
Kate and her dedicated financial services regulation team specialise in payment systems regulation, financial crime laws, sanctions laws, privacy laws and standard form documentation for financial products.
In recognition of her achievements, Kate is a ranked lawyer for Financial Services Regulation in the 2019 *Chambers & Partners Asia-Pacific Guide* and was listed as one of Australia's *Best Lawyers* from 2015 to 2019 in the Banking and Finance division.

**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

**Amelia Jamieson** is a Senior Associate in King & Wood Mallesons' financial services regulation team, specialising in anti-money laundering and counter-terrorism financing, financial services licensing and payments.
Amelia works with Australian banks, global financial institutions and fintechs, advising on market entry, product design, licensing and regulatory compliance. Complementing her regulatory expertise, Amelia has also designed a number of AML/CTF regtech tools for clients, which streamline and automate KYC, risk assessments and IFTI reporting.
Amelia works regularly with clients to help design and implement their AML/CTF Programs, ensuring they comply with the AML/CTF Rules and address the money laundering and terrorism financing risks the clients face.
Before joining King & Wood Mallesons, Amelia worked in the Royal Bank of Canada's global AML policy team in the bank's Toronto headquarters.

**King & Wood Mallesons**
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

# Belgium


Françoise Lefèvre


Rinaldo Saporito

Linklaters LLP



## 1 The Crime of Money Laundering and Criminal Enforcement

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

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

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

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

- **Article 505, 1st indent, 2°, of the Belgian Criminal Code (hereafter, the "BCC")**, incriminates the acts of buying, receiving, exchanging, possessing, keeping or managing assets derived from a predicate offence, but only if the agent knew or ought to have known, at the outset of each operation, that the assets derived from an illicit origin.
  A third party (i.e. a person who is not the owner of the illicit assets) can also be prosecuted on the grounds of this provision, unless the illicit assets are derived from a "simple" tax fraud.
  Case law outlines that the author of the predicate offence may not be prosecuted on the grounds of this provision unless the said predicate offence has been carried out abroad and may not be prosecuted in Belgium.
- **Article 505, 1st indent, 3°, BCC**, incriminates the acts of converting or transferring assets derived from a predicate offence. *Mens rea* is in this case more specific than under article 505, 1st indent, 2°, BCC: there must be evidence that the agent acted with the intent to conceal the illicit origin of the funds or to help any person involved in the predicate offence to avoid the legal consequences of his/her acts.
  Both the agent that has committed the predicate offence and a third party can be prosecuted on the grounds of this provision.
- **Article 505, 1st indent, 4°, BCC**, incriminates the acts of concealing or disguising the nature, the origin, the location, the disposition, the movements or the ownership of the assets derived from a predicate offence. The conduct referred to in this provision is particularly extensive, so much so that it overlaps with most of the acts incriminated under the other branches of article 505 BCC. *Mens rea* is understood as broadly as under article 505, 1st indent, 2°, BCC: the agent may be prosecuted only if he/she knew or ought to have known that the assets derived from an illicit origin.
  Both the agent that has committed the predicate offence and a third party can be prosecuted on the grounds of this provision. However, and as under article 505, 1st indent, 2°, BCC, the latter may not be prosecuted if the illicit assets derive from a "simple" tax fraud.

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

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

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

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

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

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

See question 1.1.

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

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

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

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

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

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

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

As from November 2020, enforcement will be carried out at national as well as European level, in cases where money laundering has been committed on assets originating from the European Union, with entry into force of the European Public Prosecutor. There are no parallel state or provincial criminal offences.

The Belgian law on the European Investigation Order entered into force in 2017. This measure allows for increased cooperation between investigative authorities of Member States and authorises them to use in national criminal proceedings evidence gathered in other Member States.

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

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 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, this has happened.

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

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

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

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

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

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

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

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

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

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

Yes, see questions 2.1 and 2.2 above.

### 2.4 Are there requirements only at national level?

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

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

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

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

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

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

There is no statute of limitations for administrative sanctions.

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

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

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

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

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

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

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

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

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

a) No, they are not.
b) Yes, they have.

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

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

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

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

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

Anti-money laundering requirements do not yet exist in Belgium for the cryptocurrency industry. Belgium was expected to implement the 5th AML Directive by 10 January 2020, which compels Member States to designate virtual currency exchange platforms as obliged entities. A preliminary draft bill was adopted by the Belgian Council of Ministers on 7 February 2020 and has been transmitted to the European Central Bank, the Belgian Data Protection Authority and the Belgian Council of State for their opinion.

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

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

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

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

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

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

See question 3.4.

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

See question 3.4.

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

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

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

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

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

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

**3.9 What is the criteria for reporting suspicious activity?**

Obliged entities must report all the funds, operations or facts which they suspect or have reasonable grounds to suspect are linked to money laundering. This obligation to report does not entail an obligation for the obliged entities to identify the predicate offence. They must also report all suspicious funds, operations or facts in the framework of their activities in another EEE Member State, even when they do not own in such state a subsidiary, a branch or any other kind of establishment through agents or distributors (article 47 *et seq.*).

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

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

The 18 September 2017 Act has empowered the government to create a Registry of beneficial owners which is accessible to competent authorities, FIUs and obliged entities within the framework of customer due diligence, and any person or organisation that can demonstrate a legitimate interest (article 73 *et seq.*). The practical and procedural aspects of the Registry of beneficial owners have been laid out in the Royal Decree of 30 July 2018 relating to the "UBO" Registry. Obliged entities should have registered their beneficial owners before 30 September 2019; any failure to do so could be sanctioned by a fine of a maximum of €50,000.

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

This is indeed the case.

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

No, it is not.

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

Anti-money laundering requirements are only imposed on obliged entities, which were defined in question 2.1.

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

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

## 4 General

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

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

Directive 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, was adopted on 20 June 2019 and entered into force on 11 July 2019. It aims at enhancing the use of financial information by giving law enforcement authorities direct access to information about the identity of bank account holders contained in national centralised registries. It also provides them with the possibility to access certain information from FIUs – including data on financial transactions – and also improves the information exchange between FIUs as well as their access to law enforcement information necessary for the performance of their tasks. This Directive must be implemented by 1 August 2021.

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

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

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

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

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

Directive 2018/1673 is available in English at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN.

Directive 2019/1153 is available in English at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1153&from=EN.

**Françoise Lefèvre** is a specialist in domestic and cross-border litigation and national and international arbitration.
She has extensive experience in white-collar crime investigations, regulatory investigations, corporate litigation, banking and construction law.

**Linklaters LLP**
rue Brederode, 13
1000 Brussels
Belgium

Tel: +32 2501 9415
Email: francoise.lefevre@linklaters.com
URL: www.linklaters.com

**Rinaldo Saporito** 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 LLP**
rue Brederode, 13
1000 Brussels
Belgium

Tel: +32 2501 9073
Email: rinaldo.saporito@linklaters.com
URL: www.linklaters.com

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.

**www.linklaters.com**

# Brazil


Joyce Roysen

Veridiana Vianna Chaim

Joyce Roysen Advogados


## 1 The Crime of Money Laundering and Criminal Enforcement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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* – COAF), which is the financial intelligence unit that was recently attached to the Central Bank (article 2 of Law 13,974/2020) 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.

**1.9 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 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?**

With the recent inclusion of Law 13,964/2019 in the Brazilian legal system, there is a possibility for the Public Prosecutor to propose a non-prosecution agreement for money-laundering crimes (article 28-A of the Criminal Procedure Code). To have the right to such agreement, the defendant must undertake to confess, repair the harm, give up the assets and rights arising from the crime, perform community service, pay a monetary fine and comply with other conditions to be stipulated by the Prosecutor's Office. In general, these proceedings are under judicial secrecy.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

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

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

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

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

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

**2.4 Are there requirements only at national level?**

No. Brazil is a signatory to various international treaties and conventions that establish the parameters regarding this matter, in particular: (i) the Vienna Convention of 1988, promulgated domestically through Decree 154/1991, specifically to fight and prevent money laundering in cases of drug trafficking; (ii) the Palermo Convention of 2000, promulgated domestically through Decree 5,015/2004, which deals with mechanisms to control money laundering as a way of fighting terrorism; and (iii) the Merida Convention of 2003, promulgated domestically through Decree 5,687/2005, which deals with fighting corruption and establishes regulations related to institutions commonly used for this crime. Additionally, Brazil observes the 40 Recommendations of the FATF-GAFI, a group it has been part of since 2000, guiding the formation of internal control legislation and mechanisms.

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

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

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

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

Thereafter, the duty of compliance was expressly included in the law through article 10 of Law 9,613/98, as amended by Law 12,683/12, which provides that all the persons mentioned in its article 9 must adopt policies, procedures and internal controls that allow them to identify clients and communicate their transactions and operations, if necessary. The duty of compliance thereby established covers, at the administrative level, the government agencies and authorities with jurisdiction listed in article 9 of Law 9,613/98, as well as the individuals connected to them, through this law's broad implementation.

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

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

In Brazil, the COAF, which was established by Law 9,613/98 and recently attached to the Central Bank (article 2 of Law 13,974/2020), is the Financial Intelligence Unit (FIU) responsible for receiving, storing and organising information, as well as helping fight money laundering through strategic planning.

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

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

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

The administrative penalties range from a warning to fines and the cancellation or suspension of authorisation to perform certain activities. Article 12 of Law 9,613/98 lists the penalties. Monetary fine amounts are: (i) twice the value of the transaction; (ii) twice the actual profit obtained or that presumably would have been obtained by performing the transaction; or (iii) BRL 20 million.

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

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

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

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

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

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

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

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

An administrative decision issued by the COAF in an administrative proceeding established by the executive committee of the Brazilian Central Bank that can be appealed to the chairperson of the National Financial System Appeals Board (*Conselho de Recursos do Sistema Financeiro Nacional* – CRSFN) which is the unit that serves as the final administrative appeals board (article 6 of Law 13,974/2020).

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

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

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

Article 9 of Law 9,613/98 establishes the activities subject to permanent monitoring by the corresponding legal entity, which is required to inform the COAF of all suspicious transactions for the purpose of fighting money laundering, with these being referred to as persons subject to the control mechanism.

Legal entities that perform activities related to the following items in Brazil are subject to these obligations: raising, brokering and investing third-party financial resources; and the purchase and sale of foreign currency or gold, instruments or securities. The following are also bound by these obligations:

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

In turn, articles 10 and 11 of Law 9,613/98 state the obligations that must be observed by the institutions subject to oversight:

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

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

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

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

Normative Instruction 899 was recently issued by Brazilian Federal Revenue, which institutes and governs the requirement to provide information concerning transactions with crypto assets to the Special Secretariat of Brazilian Federal Revenue. The requirement to provide information applies to: natural persons and legal entities that conduct any transactions with crypto assets related to the purchase and sale, exchange, donation or transfer of a crypto asset to an exchange; the withdrawal of a crypto asset from an exchange; temporary assignment (rent); payment in kind; issuance; and other transactions that result in the transfer of crypto assets.

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

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

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

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

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

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

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

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

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

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

Article 10 of Law 9,613/98 establishes that a person subject to the control mechanisms must identify their clients, keeping an updated record, under the terms of the proper normative instructions, and also requires: that records be kept of every transaction in domestic or foreign currency, instruments or securities, credit instruments, metals or any asset that can be converted into money that exceeds a limit established by the authority with jurisdiction and under the instructions issued by it; that the requirements of the COAF be met; that policies, procedures and internal controls compatible with the scale and volume of transactions be adopted; and that an updated registration be created and maintained at the regulatory or oversight agency or, if there is none, at the COAF, with the requirements formulated by the COAF regarding the frequency, manner and conditions being observed, and with the confidentiality of the information provided being preserved under the terms of the law. Moreover, there are specific requirements for certain types of client, such as those who are referred to as politically exposed persons, who as a rule hold public positions, and are listed in COAF Resolution 29 of December 7, 2017.

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

Shell banks are mentioned in article 52(4) of Decree 5,687 of 2006, which establishes that Brazil will apply appropriate and effective measures, with the assistance of its regulatory and supervisory agencies, to impede the establishment and activity of banks that do not have an actual presence and that are not affiliated with a financial group subject to regulation. This measure seeks to prevent the crime of money laundering. The largest Brazilian financial institutions have a prevention plan and prohibit relationships with shell banks.

**3.9 What is the criteria for reporting suspicious activity?**

Article 11 of Law 9,613/98 establishes that a person subject to the control mechanism must report to the COAF, within 24 hours, a proposal for or conduct of: any transaction in domestic or foreign

currency, instruments or securities, credit instruments, metals or any asset that can be converted into money, that exceeds the limit established by the authority with jurisdiction; and transactions that could be serious evidence of the crime of money laundering.

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

Yes. Article 10-A of Law 9,613/98, as well as Law 10,701/2003, establishes that the Brazilian Central Bank will maintain a centralised registry as a general record of account holders and clients of financial institutions, as well as their attorneys-in-fact. The data available for consultation are: identification of the client, its legal representatives and attorneys-in-fact; financial institutions at which the client maintains its assets and/or investments; beginning date; and, if any, ending date of the relationship. Data from this record can be requested by the courts, parliamentary inquiry committees, the COAF and other authorities, when duly authorised and empowered to request information. Information about companies' legal representatives and attorneys-in-fact can be obtained in public databases, such as those of the boards of trade.

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

Yes. Brazilian Central Bank Circular 3,461 establishes that financial institutions must adopt measures allowing them to confirm their clients' registration information and identify the final beneficiaries of transactions. Information about account activities and bank transactions cannot be shared between financial institutions because it is confidential. It can be shared with the COAF and police and court authorities when they are duly authorised and empowered to request information.

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

Brazilian law does not allow bearer shares for financial institutions or share corporations. Additionally, financial institutions are required to provide all the information about their shareholders and family members to the Brazilian Central Bank.

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

Yes, as described in question 3.1, not only financial institutions are subject to the control mechanisms for money laundering.

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

As described in question 3.1, not only financial institutions are subject to the control mechanisms for money laundering. However, there is no special requirement to fight money laundering that applies to free trade zones.

## 4 General

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

Bill 72/2019, which was introduced in the Chamber of Deputies, is currently being considered. It seeks to amend Law 9,613/98 and extend the same obligations that financial institutions are subject to in relation to fighting money laundering to Brazilian political parties, particularly the identification of donors and the duty to report financial 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?**

To comply with GAFI/FATF recommendations, Brazil has promulgated Law 12,683/12, which amended Law 9,613/98 and did not provide an exhaustive list of predicate offences to money laundering. It has also promulgated new antiterrorism legislation (Law 13,170/15 and Law 13,260/16). Moreover, the Ministry of Justice and Public Safety, the Solicitor General, the COAF and the Ministry of Foreign Affairs have worked to prepare a bill making United Nations Security Council sanctions directly applicable within Brazil, with the administrative freezing of assets tied to persons and entities listed by it.

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

As a full GAFI/FATF member, Brazil has made a commitment to submit to the periodic mutual evaluation process. The IMF also prepares an annual report on the Brazilian economy, which is referred to as "article IV", and this report points out instances of Brazil's progress or failure in relation to fighting money laundering.

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

Special legislation concerning money laundering can be found on the website of the office of the Brazilian president (http://www.planalto.gov.br), which contains updated official legislation. The same website has the Brazilian Penal Code, which contains the institutes that apply to money-laundering legislation. The rules of the COAF are available on its website (http://www.coaf.fazenda.gov.br/). Other government agencies that help fight money laundering can also be accessed on the internet: http://idg.receita.fazenda.gov.br/sobre/acoes-e-programas/combatea-ilicitos/lavagem-de-dinheiro; and http://www.bcb.gov.br/pt-br/#!/n/LAVAGEMDINHEIRO.

**Joyce Roysen**

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 (89.038), Member of the São Paulo Lawyers' Association and Member of the Portuguese Bar Association since 2020 (62255L). 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 2019. Recognised by *Chambers Latin America* 2017/2018/2019 as an outstanding lawyer in the field of business criminal law (Dispute Resolution Brazil – White-Collar Crime).

**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

**Veridiana Vianna Chaim** is a partner at Joyce Roysen Advogados (JRADVS) and graduated from the Pontifical Catholic University of São Paulo (PUC-SP) with a law degree in 2008. She also has a graduate degree in criminal law and procedure from the PUC-SP, having graduated in 2012. She is a Member of the Brazilian Bar Association, the Brazilian Institute of Criminal Science and of the São Paulo Lawyers' Association. She was recognised as an admired criminal law attorney by the magazine *Análise Advocacia* from 2017 to 2019.

**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

The firm Joyce Roysen Advogados was founded in 1993 and 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.

**www.jradvs.com.br**

JOYCE ROYSEN ADVOGADOS

# Canada


Katie Patterson


Vladimir Shatiryan

Blake, Cassels & Graydon LLP

## 1 The Crime of Money Laundering and Criminal Enforcement

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

Section 462.31 of the Criminal Code (Canada) creates the criminal offence of money laundering.

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

To establish money laundering as a criminal offence, the government must prove, beyond a reasonable doubt, that a person:

1. used, transferred the possession of, sent or delivered to any person or place, transported, transmitted, altered, disposed of or otherwise dealt with, in any manner and by any means, any property or proceeds of any property;
2. with intent to conceal or convert that property or those proceeds; and
3. knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of:
   a. the commission in Canada of a designated offence; or
   b. an act or omission anywhere that, if it occurred in Canada, would have constituted a designated offence.

Subject to certain exceptions, a "designated offence" is any indictable offence that may be prosecuted under the Criminal Code or any other federal Act, or any conspiracy, attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an indictable offence. Tax evasion is a designated offence, as it may be prosecuted on indictment.

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

Money laundering of the proceeds of foreign crimes is punishable under the Criminal Code where the foreign crime, if it had occurred in Canada, would have constituted a designated offence.

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

The Public Prosecution Service of Canada initiates and conducts federal prosecutions of the money-laundering criminal offence.

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

Section 462.31 applies to "every one", which includes an organisation.

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

If the offence of money laundering proceeds by indictment, the maximum penalty is imprisonment for a term not exceeding 10 years. If the offence proceeds summarily, the maximum penalty is a fine of not more than CAD$5,000 or a term of imprisonment not more than two years less a day, or both.

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

If the offence of money laundering proceeds summarily, no proceedings can be instituted more than 12 months after the time when the subject matter of the proceedings arose, unless the prosecutor and the defendant agree otherwise. If the offence proceeds by indictment, there is no statute of limitations for money-laundering crimes.

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

The offence of money laundering, as all criminal offences, is prosecuted at the federal level.

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

Section 462.37 of the Criminal Code allows a court to order the

forfeiture of certain property. This provision applies if an offender is convicted of a designated offence, but may also apply if the offender is discharged by the court after pleading guilty to or being found guilty of a designated offence. To impose a forfeiture order, the court must be satisfied, on a balance of probabilities, that the property is the proceeds of crime obtained through commission of the designated offence. If the court is not satisfied that the property was obtained through commission of the designated offence, a forfeiture order may still be made if the court is satisfied, beyond a reasonable doubt, that the property is the proceeds of crime. Property may also be forfeited by order of the court upon sentencing of an offender convicted of certain offences.

Some Canadian provinces have also enacted legislation that enables forfeiture of proceeds of crime through civil enforcement.

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

To our knowledge, there are no convictions of regulated financial institutions or their directors or officers for committing the offence of money laundering under the Criminal Code.

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

The result of negotiations between an accused and the prosecution can be public if those negotiations result in an in-court disposition that includes a plea of guilty. If the prosecution withdraws the charge or agrees to a much less onerous sentence, the result of such negotiations may not be public because they are the result of in-chambers discussions and would not form part of the public record.

Whether certain information is publicly available is very fact-dependent.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

Federally, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) imposes anti-money laundering requirements on financial institutions and certain other businesses. The PCMLTFA requires such institutions to maintain a compliance programme, appoint a compliance officer, and conduct an assessment of money-laundering and terrorist-financing risks. Further, the PCMLTFA outlines rules relating to recordkeeping, identity verification, ongoing monitoring and reporting. The PCMLTFA also requires money services businesses to register with FINTRAC, the government entity that administers the PCMLTFA.

In Quebec, the Money-Services Businesses Act (MSB Act) imposes a parallel regulation of money services businesses. The MSB Act requires money services businesses to be licensed with the *Autorité des marchés financiers*, the regulatory authority that administers the MSB Act.

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

The Investment Industry Regulation Organization of Canada (IIROC) is the national self-regulatory organisation that oversees all investment dealers and trading activity on debt and equity marketplaces in Canada. IIROC imposes client identification requirements on its members. Provincial law societies also impose anti-money laundering requirements on their member legal professionals.

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

Please see our answer to question 2.2 above.

**2.4 Are there requirements only at national level?**

Yes, the requirements are at the federal level, except in respect of money services businesses, which are also subject to provincial regulation in the province of Quebec.

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

FINTRAC is responsible for the examination for compliance and enforcement of the PCMLTFA at the federal level. In February 2019, FINTRAC published an Assessment Manual, which outlines FINTRAC's methods for selecting entities for compliance examinations and the process that FINTRAC will follow during examinations. In August 2019, FINTRAC published additional guidance which outlines its interpretation of the harm done by a violation of the PCMLTFA. The harm done by a violation factors into FINTRAC's determination of a penalty.

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

FINTRAC is responsible for analysing information reported by financial institutions and businesses subject to the PCMLTFA.

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

Administrative enforcement actions may not be commenced later than two years after the subject matter of the proceedings became known to FINTRAC. Criminal offences under the PCMLTFA may only be instituted within five years after the time when the subject matter of the proceedings arose if such offences are prosecuted summarily.

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

The maximum administrative penalty for failure to comply with a requirement of the PCMLTFA is CAD$100,000, if the violation is committed by an individual, and CAD$500,000, if the violation is committed by an entity.

The administrative penalties vary depending on whether the violation is minor, serious, or very serious. A minor violation may result in a penalty of up to CAD$1,000, a serious violation may result in a penalty of up to CAD$100,000, and a very serious violation may result in a penalty of up to CAD$500,000.

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

In addition to monetary penalties, FINTRAC may also enter into compliance agreements with persons or entities who have committed a violation.

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

Violations of anti-money laundering obligations may be subject to criminal sanctions under the PCMLTFA if a person or entity knowingly contravenes certain legislative requirements. However, criminal sanctions are rarely pursued in practice. FINTRAC's preferred enforcement tool is the administrative monetary penalties regime.

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

If FINTRAC believes on reasonable grounds that a person or entity has committed a violation, FINTRAC may issue a notice of violation. The notice of violation will state the penalty that FINTRAC proposes to impose, and may also contain an offer to reduce by half the penalty proposed in the notice if the person or entity enters into a compliance agreement with FINTRAC.

The person or entity may choose to pay the penalty, in which case the person or entity is deemed to have committed the violation and the proceedings in respect of it are ended.

Alternatively, the person or entity may make representations to the Director of FINTRAC and the Director will decide whether the person or entity committed the violation. If the violation is serious or very serious, a person or entity will have the right to appeal the Director's decision to the Federal Court of Canada within 30 days after the notice of decision is served.

FINTRAC is generally required to make public the nature of the violation or default, the name of the person or entity and the amount of the applicable penalty.

Entities subject to the PCMLTFA have challenged penalty assessments issued by FINTRAC in the Federal Court of Canada from time to time.

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

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

The PCMLTFA applies to the following types of persons and entities:

1. banks and foreign bank branches;
2. credit unions and centrals;
3. life companies;
4. trust and loan companies;
5. securities dealers;
6. domestic money services businesses and, effective as of June 1, 2020, foreign money services businesses;
7. intermediaries engaging in certain activities, such as life insurance brokers and agents, British Columbia notaries public and notary corporations, legal counsel and legal firms (subject to limitations), accountants and accounting firms, real estate brokers, sales representatives and developers, and dealers in precious metals and stones; and
8. casinos.

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

The federal government has introduced amendments to the definition of "money services business" in the PCMLTFA to include persons engaged in the business of dealing in virtual currencies. These amendments will come into force on June 1, 2020. The federal government has also introduced amendments to the PCMLTFA regulations which will impose various identification, reporting and recordkeeping requirements on persons dealing in virtual currencies. These amendments are scheduled to come into force on June 1, 2021.

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

All persons and entities that are subject to the PCMLTFA must establish and implement a compliance programme. As part of the compliance programme, they must:

1. appoint an anti-money laundering officer;
2. develop and apply written compliance policies and procedures;
3. conduct and document risk assessment;
4. develop and maintain a written, ongoing compliance training programme for employees and agents; and
5. conduct and document an effectiveness review of the policies and procedures, the risk assessment and the training programme. This review must be carried out every two years by an internal or external auditor.

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

Subject to certain exceptions, persons and entities that are subject to the PCMLTFA must report and keep a record of a transaction where they receive from a client an amount in cash of CAD$10,000 or more in the course of a single transaction, unless the amount is received from a financial entity or a public body. A "single transaction" will include two or more cash transactions of less than CAD$10,000 each if they are made within 24 consecutive hours and total CAD$10,000.

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

Financial entities, money services businesses and casinos must report the sending out of Canada, or the receipt from outside Canada, of international electronic funds transfers of CAD$10,000 or more in the course of a single transaction.

Electronic funds transfers that are sent to a person or entity within Canada do not have to be reported, even if the final recipient is outside Canada. Similarly, electronic funds transfers that are received from a person or entity within Canada do not have to be reported, even if the initial sender is outside Canada. For SWIFT messages, only SWIFT MT 103 messages are reportable.

Casinos are also required to report large disbursements of CAD$10,000 or more.

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

Please see our answer to question 3.5 above.

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

Financial institutions are required to conduct customer identification when opening an account for a customer and for certain threshold transactions. For individuals, customer identification must be conducted using in person or non-face-to-face methods prescribed by legislation and discussed in FINTRAC guidance. For entities, customer identification is conducted by confirming the entity's legal existence and identifying its authorised signers. Financial institutions are also required to determine an entity's ultimate beneficial owners. The customer identification requirements for other businesses subject to the PCMLTFA are largely similar.

Customers that are assessed to be higher risk must be subject to enhanced customer identification and ongoing monitoring requirements. These enhanced measures may differ depending on the customer.

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

Yes. No person or entity may have a correspondent banking relationship with a shell bank, which is defined as a foreign financial institution that does not have a physical presence in any country, unless it is controlled by or is under common control with a depository institution, credit union or foreign financial institution that maintains a physical presence in Canada or in a foreign country.

**3.9 What is the criteria for reporting suspicious activity?**

Regulated persons or entities must report to FINTRAC every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or the attempted commission of a money-laundering or terrorist activity-financing offence. "Reasonable grounds to suspect" is a conclusion that is reached based on an assessment of facts, context and money-laundering/terrorist-financing indicators. "Reasonable grounds to suspect" is a step higher than "simple suspicion" (i.e., a "gut feeling" or "hunch") and a step below "reasonable grounds to believe" (i.e., there is a probability, supported by verified facts, that a money-laundering or terrorist activity-financing offence has occurred), according to FINTRAC.

Persons and entities may not disclose (1) that they have made, are making or will make a suspicious transaction report, or (2) the contents of a suspicious transaction report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.

A person or an entity is not liable to criminal or civil proceedings for making a suspicious transaction report in good faith or for providing FINTRAC with information about suspicions of money laundering or of the financing of terrorist activities.

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

There is no public registry of beneficial ownership information at the federal or provincial level. The Government of Canada intends to work with the provinces and territories to create a pan-Canadian beneficial ownership registry for all legal persons and entities, including trusts, who have 25% of total share ownership or voting rights. It is not yet clear whether the registry will be publicly available. The federal and British Columbia governments have recently amended their corporate statutes to require corporations to record individuals with significant control in a transparency registry.

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

Financial entities, money services businesses and casinos must include with an electronic funds transfer the name, address and

account number or other reference number, if any, of the person who requested it. This requirement applies to electronic funds transfers, including transfers within Canada that are SWIFT MT 103 messages. Such entities must also take reasonable measures to ensure that any transfer that the person or entity receives includes that information.

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

The Canada Business Corporations Act prohibits the issuance, in bearer form, of a certificate, warrant or other evidence of a conversion privilege, option or right to acquire a share of a federal corporation.

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

As noted in our answer to question 3.1 above, the PCMLTFA applies to certain non-financial institution businesses, such as British Columbia notaries, legal counsel and law firms (subject to limitations), accountants and accounting firms, real estate brokers or sales representatives, dealers in precious metals and stones, real estate developers and casinos.

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

No, but under Part 1.1 of the PCMLTFA, the Minister of Finance can issue Directives to safeguard the integrity of Canada's financial system. On December 9, 2017, the Minister of Finance issued a Directive on the Democratic People's Republic of Korea, which requires reporting entities to treat all transactions originating from or destined to North Korea as high risk.

## 4 General

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

In June 2019, the federal government released substantial amendments to the PCMLTFA regulations. The amendments expand the PCMLTFA's application to virtual currencies, businesses providing foreign money services and pre-paid products, among other measures. The majority of the amendments will come into force on June 1, 2021, with the exception of a small number of changes, which will take effect on June 1, 2020.

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

In 2016, the FATF released its report discussing its detailed assessment of Canada's anti-money laundering framework. The report concluded that Canada has a strong anti-money laundering and anti-terrorism regime, but requires improvements to be fully effective. The report noted that constitutional constraints limit the ability to fully cover all high-risk areas, such as legal counsel, law firms and Quebec notaries. The report also noted that further supervisory efforts are necessary with respect to the real estate and dealers in precious metals and stones sectors.

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

As noted above, the FATF released its report discussing its detailed assessment of Canada's anti-money laundering framework in 2016.

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

The following legislation and administrative guidance is available online:

1. The Criminal Code.
2. The PCMLTFA (and its associated regulations: Cross-border Currency and Monetary Instruments Reporting Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations, Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, and Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations).
3. The Money-Services Businesses Act (Quebec) (and its associated regulations: Regulation under the Money-Services Businesses Act, and Regulation respecting fees and tariffs payable under the Money-Services Businesses Act).
4. FINTRAC Guidance.
5. OSFI Guideline B-8: Deterring and Detecting Money Laundering and Terrorist Financing.
6. *Autorité des marchés financiers* Guidance.

**Katie Patterson**'s practice focuses on regulatory compliance for federally and provincially regulated financial institutions. She advises a variety of financial service providers, including Canadian and foreign banks, insurance companies, credit unions, money services businesses and commercial and consumer finance companies.

**Blake, Cassels & Graydon LLP**
199 Bay Street, Suite 4000
Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: +1 416 863 2659
Email: katie.patterson@blakes.com
URL: www.blakes.com

**Vladimir Shatiryan**'s practice focuses on a broad range of issues impacting Canadian and foreign financial institutions, including banks, insurance companies, credit unions, financial market infrastructures and payment service providers. He advises on business and ownership structures, establishment of financial institutions and foreign bank branches, cross-border banking rules, permitted investments and activities, bank resolution and recovery laws, regulatory compliance management and governance, payment clearing and settlement laws, and other regulatory issues. Vladimir also has expertise in all aspects of Canada's anti-money laundering legislation and sanctions legislation. Vladimir has completed a secondment at the Legislation and Approvals Division of Canada's federal banking regulator, the Office of the Superintendent of Financial Institutions.

**Blake, Cassels & Graydon LLP**
199 Bay Street, Suite 4000
Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: +1 416 863 4154
Email: vladimir.shatiryan@blakes.com
URL: www.blakes.com

As one of Canada's top business law firms, Blake, Cassels & Graydon LLP (Blakes) provides exceptional legal services to leading businesses in Canada and around the world. Thanks to our clients, Blakes has been named the leading law firm brand for the fifth consecutive year in the Acritas Canadian Law Firm Brand Index 2020. Blakes received the most top-tier rankings by practice area of any law firm for the third year in a row, according to *Chambers Canada: Canada's Leading Lawyers for Business 2020*, and was named one of Canada's Best Diversity Employers by Mediacorp Canada Inc. for the 10th time. Blakes is recognised as having Canada's pre-eminent financial services practice, including the largest and most active financial services regulatory practice in the country. We provide sophisticated advice to numerous regulated financial institutions, as well as commercial and consumer finance companies, operators of payment systems and other financial service providers, fintechs, intermediaries, and distributors. We have extensive experience advising all entities subject to Canadian anti-money laundering, anti-terrorist financing and economic sanctions legislation applicable to financial transactions.

**www.blakes.com**

# 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 the national level?

The People's Procuratorate is the 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?

Money laundering is a criminal offence under Article 191 of the PRC Criminal Law ("**Criminal Law**"). To establish a crime of money laundering against an offender, the prosecutor shall prove with irrefutable evidence that: (i) there are proceeds generated from predicate offences; and (ii) there are intentions and acts of the offender to dissimulate or conceal the source/nature of such proceeds.

**Predicate offences**

Money laundering predicate offences refer to criminal activities in relation to: (i) drugs; (ii) organised crime; (iii) terrorism; (iv) smuggling; (v) corruption & bribery; (vi) disruption of the financial regulatory order; and (vii) financial fraud.

Tax evasion is not a predicate offence of the crime of money laundering. Nevertheless, dissimulating or concealing proceeds generated by the crime of tax evasion will be charged under a separate crime (i.e. 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 find of 20% of the amount of laundered money. For an institution, the maximum penalty is a criminal fine of 20% of the amount of laundered money with its directly responsible personnel subject to imprisonment for a fixed term of 10 years.

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

The statute of limitations for money laundering crimes is 15 years starting from the conclusion of criminal activities.

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

The *Criminal Law* is the only criminal code in the PRC and shall be applicable and enforceable across the whole country.

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

If a confiscation decision is made by a court, such court is the confiscation authority, and, when necessary, such court may require assistance from the public security authorities in enforcing the confiscation decision. If a confiscation decision is made by an administrative authority, the authority making such decision is the confiscation authority.

For a crime of money laundering, all criminal proceeds and gains obtained in relevant criminal activities are subject to confiscation.

If a People's Procuratorate decides not to prosecute a crime of money laundering but deems the relevant funds shall be subject to non-criminal confiscation, such People's Procuratorate shall form an opinion and hand over the case to another relevant administrative authority (e.g. the PBOC (as defined below)) for further handling.

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

We found, in most instances, employees of banks or other regulated financial institutions that have been involved in money laundering activities would be convicted under separate crimes (e.g. the crime of corruption, which has a higher maximum sentence). Please note that decisions of PRC courts 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?**

The crime of money laundering 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* systematically set out 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 Entities**").

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 of AML Reporting Entities in conducting their business (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 ("**CBIRC**"), and the 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*).

As a high-level summary, you may find PRC AML requirements as follows (note: this is not a complete list):

i. Customer identity verification obligation – all AML Reporting Entities shall:
   a) require their customers to provide valid identity certificates;
   b) regularly review and continuously monitor their customers' identities; and
   c) re-identify their customers upon the occurrence of certain changes.
ii. Customer identity and transaction records-keeping obligation – all AML Reporting Entities shall:
   a) retain copies of their customers' identity certificates;
   b) keep records of their customers' identity information; and
   c) maintain records of their customers' transactions.
iii. Reporting obligations – all AML Reporting Entities shall timely report to the local PBOC office and the AML Data Center (as defined below) if:
   a) their customers refuse to provide valid identity certificates;
   b) their customers act suspiciously or any transaction is suspicious; and
   c) the amount of any transaction exceeds the thresholds set out by the authority.
iv. Other obligations – all AML Reporting Entities shall:
   a) have a special department to be in charge of all AML issues;
   b) establish a complete AML internal control system; and
   c) organise AML training, etc.

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

There are AML requirements imposed by self-regulatory organisations.

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

Within their authorities, self-regulatory organisations are responsible for AML compliance and enforcement against their members.

**2.4 Are there requirements only at national level?**

All requirements mentioned here shall be applicable at all levels.

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

The PBOC is the regulatory authority responsible for the compliance and enforcement of AML requirements. Besides, the CBIRC and the CSRC are responsible for ensuring relevant financial institutions have established complete AML internal control systems and assisting the PBOC in enforcing certain administrative sanctions.

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

The China Anti-Money Laundering Monitoring & Analysis Center ("**AML Data Center**"), run by the PBOC, is the FIU responsible for analysing information reported by all AML Reporting Entities.

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

The applicable statute of limitations for competent authorities to bring administrative enforcement actions against AML violators is two years starting from the conclusion of the violations.

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

The maximum administrative fine on an AML Reporting Entity for failure to comply with 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 AML requirements is RMB 500,000 and/or such person could be subject to the revocation of his/her qualification to participate in financial activities and/or be banned from any financial related occupations.

Violations that may trigger the above penalties include but are not limited to:

- failure to establish a complete AML internal control system;
- failure to have a department in charge of AML issues;
- failure to arrange 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 an AML investigation; or
- refusal to provide AML investigation materials or providing 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 violation, it has the authority to investigate relevant AML Reporting Entities or their employees using methods such as questioning relevant persons, compelling entities to provide relevant materials, etc. After the investigation, the PBOC may choose whether or not to impose sanctions and, if so, which sanctions to impose on the relevant entities and/or persons. For violations that trigger the crime of money laundering, the PBOC will hand over the investigation to the public security authority for further handling.

Most resolutions of penalty actions, but not all, by competent authorities are publicly available on the respective competent authorities' websites.

An AML Reporting Entity or an individual may appeal an administrative decision made by a financial regulatory authority to the upper level authority for reviewing the decision or file an administrative action against such authority in a PRC court.

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

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

**Financial institutions** that are subject to AML requirements include:

- all banks and credit cooperatives;
- securities companies, futures companies and fund management companies;
- insurance companies and insurance asset management companies;
- trust & investment companies, asset management companies, finance companies, financial leasing companies, auto finance companies and money brokerage companies; and
- other financial institutions as identified by the PBOC.

**Other designated non-financial institutions** that are subject to AML requirements include:

- institutions conducting money remittance, exchange, settlement and/or clearing business;
- funds distribution institutions;
- internet financial institutions;
- real estate development companies, real estate selling agencies, other agencies that provide services in relation to real estate transactions;
- precious metal exchanges that conduct spot trading or provide services for spot trading and traders;
- accounting firms, law firms and notary agencies that handle the following business on behalf of their clients – buying and selling real estate, escrowing funds, securities or other assets, escrowing bank accounts and securities accounts, raising funds for establishment and operation of enterprises and buying and selling business entities;
- service providers that provide professional services for the establishment, operation and management of companies, act or arrange others to act as directors or partners, hold companies' shares, and provide registered addresses, office addresses or mailing addresses to companies; and
- other non-financial institutions as identified by the PBOC.

The PRC AML regime focuses more on what kind of institutions (instead of what kind of activities) shall be subject to AML requirements. There is no consolidated list of activities that are subject to AML requirements. Nevertheless, the authorities, from time to time, issue rules to emphasise AML requirements of certain activities (e.g. establishing cross-border cooperation with a foreign financial institution).

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

At the time of writing, issuing and trading cryptocurrency in the PRC is illegal and forbidden.

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

AML Reporting Entities are required to have complete AML internal control systems which shall cover all AML requirements as outlined in question 2.1.

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

In respect of recordkeeping, an AML Reporting Entity is required to keep records of all transactions for at least five years, regardless of the value of the transaction.

In respect of large cash transactions reporting, an AML Reporting Entity shall report if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 50,000 (included), or USD 10,000 (included) or the equivalent.

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

In respect of other large-value transactions, AML Reporting Entities shall also report:

- for fund transfers of institutional customers, if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 2 million (included), or USD 200,000 (included) or the equivalent;
- for onshore funds transfers of individual customers, if the value of a single transaction or the accumulated value of all transactions within a day exceeds RMB 500,000 (included), or USD 100,000 (included) or the equivalent; and
- for cross-border fund transfers of individual customers, if the value of a single transaction or the accumulated value of various transactions within a day exceeds RMB 200,000 (included), or USD 10,000 (included) or the equivalent.

AML Reporting Entities shall also report suspicious transactions (please refer to question 3.9).

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

Criteria for reporting cross-border large-value transactions are outlined in questions 3.4 and 3.5. Criteria for reporting cross-border suspicious transactions are outlined in question 3.9.

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

General customer identification and due diligence requirements for AML Reporting Entities include but are not limited to:

- for institutional customers, verifying the name, address, scope of activities, valid licences proving the lawful establishment of the institution, shareholding structure, constitutional documents (including registration certificate, partnership agreement, articles of association, etc.), information of institutional shareholder or directors, and name, valid ID of the controlling shareholder/person, beneficiary owner, legal representative, responsible manager and authorised agent; and
- for individual customers, verifying the name, gender, nationality, occupation, residence/place of working, contact and valid ID.

Enhanced customer identification and due diligence requirements for AML Reporting Entities include but are not limited to:

- for institutional customers whose shareholder is another institution, tracking down the individual who is the controlling person or beneficiary owner of such institutional customers, and verifying and registering information of each beneficiary owner;

- for institutional customers with high risk, verifying the beneficiary owner of such customers with even more stringent standards; and
- for individual customers who have special standings (e.g. senior managers of international organisation and officers of foreign countries), verifying the special standings of these customers, obtaining senior managers' approval before taking in such individuals as customers, understanding assets of such customers and sources of such assets, and enhancing the frequency and intensity of transaction monitoring.

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

All financial institutions are strictly prohibited from opening any account for or developing any cooperation with foreign banks which have no actual business activities in the countries where they are licensed and are under no effective supervision.

**3.9 What is the criteria for reporting suspicious activity?**

All AML Reporting Entities shall report suspicious transactions. Suspicious transactions refer to all transactions, regardless of the value involved, that an AML Reporting Entity has reasonable cause to believe that such transactions or any person engaged in such transactions are related to criminal activities. AML Reporting Entities shall formulate their internal transactions monitoring standards in accordance with the requirements of the law, use such standards to identify every suspicious transaction and report every identified suspicious transaction to the local PBOC office and the AML Data Center.

Specifically, all AML Reporting Entities must report a transaction if the transaction:

- is related to money laundering, terrorism financing or other criminal activities;
- will jeopardise national security or social stability;
- is linked to other serious situations or emergencies; or
- is related to anyone on the list of terrorism organisations and terrorists as published by the PBOC, the United Nations Security Council, or other organisations that the PBOC requires all entities to pay attention to.

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

The State Administration for Market Regulation maintains current and adequate institutional information of all corporates established within the PRC. Other authorities also publish information of special licences approved by such authorities.

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

Accurate information about originators and beneficiaries must be included in payment orders for all fund transfers. Such information shall also be included in payment instructions to other financial institutions.

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

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

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

There are specific AML requirements applied to non-financial institution businesses.

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

More attention is required to be paid to high-risk business sectors (e.g. international trade).

## 4 General

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

In the upcoming years, PRC AML will focus on resolving key problems and filling gaps.

**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 (2019), the FATF concluded that the PRC is able to take sufficient actions to meet most of the FATF's recommendations with few deficiencies and non-compliant points.

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

The FATF finished its scheduled onsite visit to the PRC in 2018/2019 and a new mutual evaluation report was issued 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?**

Most AML rules are available at http://www.pbc.gov.cn/fanxiqianju/135153/135173/index.html. Websites of other authorities (e.g. the State Council, CBIRC, CSRC, etc.) will also publish relevant AML laws, regulations and rules issued by the corresponding authority. These materials are not published in English, but English versions of some materials can be found on the FATF's website with other resources.

**Chen Yun** is a partner at King & Wood Mallesons specialising in banking, finance, foreign exchange and AML laws.
His practice includes general banking, financial regulatory, 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; standardising daily operational bank documentation; and assisting foreign banks in establishing, reorganising, and expanding their business presence in China.
Mr. Chen has been ranked as one of the leading individuals in banking and finance areas by *Chambers & Partners* for many years.

**King & Wood Mallesons**
17th Floor, One ICC
Shanghai ICC, 999 Huai Hai Road
Xuhui District, Shanghai 200031
China

Tel: +86 21 2412 6052
Email: chenyun@cn.kwm.com
URL: www.kwm.com/zh/cn

**Liang Yixuan** is an associate of Mr. Chen Yun at King & Wood Mallesons specialising in banking, financing, 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' products; documenting transactions; and standardising daily operational bank documentation; and assisting foreign banks in establishing, reorganising, and expanding their business presence in China.

**King & Wood Mallesons**
17th Floor, One ICC
Shanghai ICC, 999 Huai Hai Road
Xuhui District, Shanghai 200031
China

Tel: +86 21 2412 6447
Email: liangyixuan@cn.kwm.com
URL: www.kwm.com/zh/cn

# France



Alexis Gublin


Louise Lecaros de Cossio


Pierre Calderan


Thomas Bourceau

Delecroix-Gublin




## 1 The Crime of Money Laundering and Criminal Enforcement

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

The public prosecutor with each tribunal oversees the prosecution of money-laundering offences within its territorial jurisdiction. A special Prosecutor for Financial Crimes (the "PNF") has jurisdiction over money-laundering offences nationwide in cases where the laundering relates to sums obtained through the commission of certain offences such as corruption, tax fraud and misappropriation of public funds.

### 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 general offence of money laundering is provided for by article 324-1 of the Criminal Code. Special money-laundering offences also exist under the Criminal Code, the Customs Code and the Monetary and Financial Code (the "MFC").

Under article 324-1 of the Criminal Code, the government must first establish that the accused has: (1) facilitated, by any means, the fraudulent justification of the origin of the property or income of the perpetrator 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.

For both prongs of the offence, the government must establish that the accused knew of the illegal origin of the property. It is not necessary to establish that the accused had knowledge of the specific predicate crime or offence of which the profits were laundered.

Further, it must be proven that a predicate offence has been committed. However, the predicate offence need not have been prosecuted and it does not matter that prosecuting the predicate offence before French courts is impossible; for example, if the statute of limitation has run.

The burden of proof on the prosecution is lowered by article 324-1-1 of the Criminal Code. Indeed, under this provision, property or income is presumed to be the direct or indirect proceeds of an offence where the material, legal or financial conditions of the investment, concealment or conversion transaction can have no justification other than to conceal the origin or the beneficial owner of such property or income. The defendant must provide evidence that funds or property were lawfully obtained.

With the exception of petty offences, any offence may constitute a predicate to money laundering, such as tax evasion.

### 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. French courts also have jurisdiction over offences committed by a French national abroad, with a condition that the conduct must be punishable under the legislation of the country in which it was committed. Finally, French courts have jurisdiction over offences committed abroad against a French national.

Therefore, French courts have extraterritorial jurisdiction over the crime of money laundering.

French courts have held that it is not necessary for the predicate offence to be committed in France for French courts to have jurisdiction over the act of money laundering, as long as at least one of the constituent elements of money laundering was committed in France.

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

Investigations are led by the police or the gendarmerie, usually through a special division tasked with combatting fraud, money laundering and other financial crimes, either under the supervision of the local public prosecutor or the PNF.

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 the official complaint of the victim, and after the victim has confirmed their will to proceed.

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

Both legal persons and natural persons can be prosecuted and convicted for money laundering.

The liability of legal persons can only be retained based on acts committed by their officers, directors or representatives on their behalf.

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

The maximum penalties applicable to natural persons convicted of money laundering are five years' imprisonment and a fine of €375,000.

Money laundering is aggravated under certain circumstances. Penalties for natural persons convicted of aggravated money laundering are increased to 10 years' imprisonment and a fine of €750,000.

In any case, the amount of the fine may be raised up to half the value of the assets or funds involved in the laundering operations.

In cases where the predicate offence carries a term of imprisonment exceeding the term of imprisonment for money laundering, and where 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 persons convicted of money laundering, the maximum applicable penalty is a fine of €1,875,000. The maximum penalty for legal persons convicted of aggravated money laundering is a €3,750,000 fine. Penalties for legal entities may also include: dissolution or prohibition on exercising one or more social or professional activities, either permanently or for a maximum period of five years; exclusion from public procurement contracts in France on a permanent basis or for a period of up to five years; and prohibition, on a permanent basis or for a maximum period of five years, on making a public offering of financial securities or having its financial securities admitted to trading on a regulated market.

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

The statute of limitations for prosecuting money laundering is 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.

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

Enforcement is not centralised at the national level but handled by eight specialised inter-regional jurisdictions based in Paris, Lyon, Marseille, Lille, Rennes, Bordeaux, Nancy and Fort de France (the "JIRS"). The JIRS bring together prosecutors and investigating judges with experience in the fight against organised and financial crime in complex cases. The JIRS are relieved of the simpler cases that are handled by local courts.

The most complex prosecutions are led by the PNF.

France is not a federal state; therefore, the issue of parallel state or provincial criminal offences does not arise.

### 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 the event of a criminal conviction for money laundering, the court may impose a penalty of confiscation on the offender, whether a natural person or a legal entity. All assets can be subject to forfeiture, whether they are movable assets or real estate, including jointly owned property.

The Agency for the Management and Recovery of Seized and Confiscated Assets ("AGRASC") is a state public institution of an administrative nature under the joint supervision of the Minister of Justice and the Minister in charge of the Budget.

The agency is responsible for ensuring, on the basis of a court order, the management of all property, whatever its nature – seized, confiscated or subject to a protective measure in the course of criminal proceedings – which is entrusted to it and which requires administrative acts for its conservation or enhancement. The AGRASC also handles the centralised management of all sums seized during criminal proceedings.

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

Bank and financial institution directors, officers and employees are those most susceptible to criminal prosecution and conviction for money laundering. Examples include a recent case from the Paris criminal court: in February 2019, the Swiss bank UBS AG was found guilty of aggravated money laundering by the criminal court of Paris, and convicted to a fine of €3.7 billion, in addition to €800,000,000 in damages to the French State. UBS France was also found guilty of aiding and abetting money laundering and was given a €15,000,000 fine. UBS has lodged an appeal against this verdict and the appeal trial is scheduled to take place in June 2020.

### 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 proceedings for money laundering can be resolved outside of courts through settlements with the relevant authorities, if certain conditions are met.

The prosecution may offer a guilty plea (*comparution préalable sur reconnaissance de culpabilité*) where the defendant, either a natural or legal person, is charged with money laundering. The defendant must plead guilty in exchange for a reduced sentence. Terms of imprisonment cannot in any case exceed three years, 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.

It is also possible for the prosecutor to offer another type of guilty plea (*composition pénale*) to natural persons, only in cases where charges are brought for offences punishable by five years' imprisonment or less, as is the case with money laundering. Sentences available to the prosecution do not include prison terms. Therefore, charges of money laundering could be settled through a *composition pénale*, although it is unlikely considering the complexity of the facts in money-laundering cases.

Both plea-bargaining procedures must be approved by a judge in open court.

Act n°2016-1691 of December 9, 2016 introduced into French law the *Convention Judiciaire d'Intérêt Public* (the "CJIP"), a new kind of settlement resembling the existing U.S. deferred prosecution agreement, for legal entities charged with money laundering of tax evasion proceeds, corruption, influence peddling, and other specific offences.

This deal is offered by the prosecution or in cases of indictment and under certain circumstances, by an investigative judge, and may also be suggested by the company's lawyer.

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. The amount of that fine shall be set in proportion to the benefits derived from the breach of law, up to a limit of 30% of the average annual turnover calculated on the basis of the last three annual turnovers. The amount of the fine is set after a phase of negotiation between the prosecutor and the company, considering in particular the level of cooperation of the company during the investigation;
- setting up a compliance programme under the supervision of the French anti-corruption agency, for a maximum period of three years; and
- compensation for identified victims.

The deal must be approved in an open court, and records of the fact and terms of the CJIP are public and available online (at: https://www.agence-francaise-anticorruption.gouv.fr/fr/convention-judiciaire-dinteret-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.

In France, the MFC establishes, under Title VI of Book V, anti-money laundering ("AML") obligations for financial institutions and other businesses. These provisions are supplemented by other regulatory texts adopted by the Prudential Supervision and Resolution Authority (the "ACPR" – French acronym for *Autorité de contrôle prudential et de résolution*) and the Financial Markets Authority (the "AMF" – French acronym for *Autorité des marchés financiers*).

In addition, France, as an EU Member State, is under the obligation to implement the EU AML Directives in its national law. In this sense, the MFC's provisions are often revised. Since January 2020, the objectives of the 5th EU AML Directive have been incorporated into the MFC.

Concerning AML requirements, the MFC imposes the following main obligations on financial institutions and other designated businesses:

- **Customer due diligence obligation:** this obligation includes: i) identification/verification of the customer's identity; ii) identification/verification of the beneficial owner's identity; iii) obtention of information on the nature and purpose of the business relationship in order to establish a risk profile of the customer; and iv) establishment of ongoing monitoring to report risky transactions and to maintain and update customer information. The level of due diligence required depends on the level of risk of AML to which the financial institution is exposed.
- **Obligation to maintain documents and information** for five years from the account closure date or from the termination date of the business relationship.
- **Obligation to report suspicious transactions**, where applicable.
- **Obligation to implement AML procedures and policies**, as well as internal controls.

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

No; although self-regulatory organisations or professional associations may control the compliance of their members to AML requirements and sanction them in case of failure, they may not impose additional requirements. However, it should be noted that self-regulatory organisations and professional associations have often published guidelines on AML compliance for their members.

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

Yes, article L. 561-36 of the MFC lists self-regulatory organisations and professional associations responsible for AML compliance against their members. Among others, local Bar Councils, Notary Chambers, Department Chambers of Judicial Officers, and the National Association of Chartered Accountants are mentioned.

### 2.4 Are there requirements only at national level?

Yes, AML requirements are only laid down at national level following the MFC's provisions. In this sense, there are no additional requirements imposed at a smaller local level.

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

The authorities responsible for controlling compliance and enforcement of AML requirements are as follows:

- **The ACPR** is responsible for the supervision of banking and insurance institutions and their intermediaries, including credit institutions, payment institutions and electronic money institutions. The ACPR may carry out document and on-the-spot checks. The ACPR has the power to issue administrative sanctions, including non-pecuniary and pecuniary penalties. The criteria for examination as well as the ACPR's decisions and guidelines are publicly available on its web page (at: https://acpr.banque-france.fr/).
- **The AMF** is responsible for the supervision of the financial industry's players, such as asset management companies, financial investment advisors and crowdfunding intermediaries. The AMF may also conduct document and on-the-spot checks and adopt administrative measures, including non-pecuniary and pecuniary penalties. The AMF makes public its regulation as well as decisions and guidelines (at: https://www.amf-france.org/), and thus the criteria for examination are publicly available.
- **Specific supervisory authorities of self-regulatory organisations and professional associations** are responsible for the supervision of their members (such as the local Bar Councils for lawyers). Such supervisory authorities may impose non-pecuniary and pecuniary penalties. In addition, most of them publish guidelines or establish training.
- **The National Sanctions Commission** (the "CNS" – French acronym for *Commission nationale des sanctions*) is

responsible for the supervision of certain professionals who do not belong to the financial sector nor a professional order/disciplinary body, including real estate agents and betting operators. The CNS may adopt administrative measures, including non-pecuniary and pecuniary penalties. The criteria for examination, as well as CNS's decisions and guidelines, are publicly available (at: https://www.economie.gouv.fr/commission-nationale-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?**

Yes, TRACFIN (French acronym for "Treatment of Information and Action against Illicit Financial Circuits") is the French designated FIU. TRACFIN – which was created in 1990 and since 2019 has been under the authority of the Ministry of Public Action and Accounts – is the national reporting authority responsible for collecting, analysing and enriching information given by, *inter alia*, financial institutions and businesses subject to AML requirements under the MFC. TRACFIN is regulated under Book V, Title VI, Chapter I, Section 5 of the MFC.

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

There is a six-year statute of limitations for the AMF to bring enforcement actions. The starting point of this limitation period is set at the day on which the breach was committed or, if the breach is concealed or hidden, the day on which the breach appeared and was established in conditions allowing the AMF to carry out its investigation or control mission. In the latter case, the limitation period may not exceed 12 completed years. However, there is no limitation period before the ACPR or the CNS.

**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 AML requirements can lead to the following maximum administrative fines:

- up to €5,000,000 before the CNS;
- up to €5,000,000 for natural persons and €100,000,000 or 10% of the net annual turnover, whichever is highest, for legal entities, before the ACPR; and
- up to €15,000,000 or 10 times the amount of profits made for natural persons and €100,000,000 or 10 times the amount of profits made for legal entities, before the AMF.

A failure to comply with AML requirements set out in the MFC can lead to a sanction. For instance, the following acts could constitute a breach of AML obligations: failure to carry out risk assessments; or failure to report suspicious transactions, when required.

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

Both the ACPR and the AMF can adopt remedial measures. In addition, the following measures can be imposed on individuals and legal entities besides pecuniary penalties:

| | |
|---|---|
| **ACPR** | Warning, reprimand, temporary prohibition of professional activity for a period of no more than five years, and withdrawal of professional licence. |
| **AMF** | Warning, reprimand, prohibition of executing certain operations for a period of no more than 10 years, temporary suspension of directors for a period of no more than 10 years, removal of directors, and partial or total withdrawal of the licence. |
| **CNS** | Warning, reprimand, partial or total prohibition of executing certain operations, and partial or total withdrawal of the licence. |

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

Certain breaches of AML requirements imposed by the MFC can cause additional criminal sanctions. For instance, breaching the prohibition on disclosure to the public of information contained in the declaration of suspicious transactions would constitute a criminal offence.

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

a) The ACPR, AMF and CNS's decisions are publicly available (see question 2.5).

b) ACPR sanctions' decisions may be appealed in administrative proceedings before the Council of State (French Supreme Administrative Court, in French *Conseil d'Etat*). CNS's decisions may also be appealed in administrative proceedings before the Parisian administrative court (*tribunal administratif de Paris*). Concerning AMF sanctions' decisions, the Council of State (administrative proceedings) is the competent authority to hear appeals against decisions taken under article L. 621-9 II of the MFC (*e.g.*, investment service providers); for all other appeals, the competent authority is the Paris Court of Appeal (judicial proceedings).

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

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

The financial institutions and other designated businesses subject to AML requirements are listed under article L. 561-2 of the MFC.

Financial institutions refer to entities operating in the banking sector such as credit and payment institutions, electronic money institutions, insurance companies, banking operations intermediaries, the Banque de France, investment firms, and money changers.

In addition, other professional activities are subject to AML requirements such as gambling and betting operators, art and antiques dealers, accountants, lawyers, notaries, auction sellers and sport agents.

These financial institutions are subject to specific requirements such as:

- a duty of care regarding their clients;
- the obligation to report to TRACFIN any sums entered in their books or transactions involving sums that they know, suspect or have good reason to suspect derive from an offence punishable by a prison sentence of more than one year; and
- the implementation of internal controls and processes aiming at preventing money laundering and terrorism financing.

Apart from these specific requirements, the MFC requires all companies registered in France, all foreign companies having a branch in France, or any legal entity registered in France, to obtain and keep accurate and up-to-date information on their beneficial owners. These companies must communicate to the Trade and Companies Registry a document stating various pieces of information in relation to their beneficial owners.

These general requirements are not applicable to companies whose securities are admitted to trading on a regulated market in France, in the EU or in a country with similar legislation.

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

The EU Directive 2018/843 of May 30, 2018 which entered into force in France on January 20, 2020 extended some of the AML requirements to the cryptocurrency industry.

From now on, cryptocurrency exchange platforms and custodian wallet providers must, like banks, apply customer due diligence controls, including customer verification requirements. In practice, they have a duty of care regarding the identity of their clients and the origin of their clients' money.

In addition, these platforms and providers will also have to be registered, as will currency exchanges and cheque-cashing offices, and trust or company services providers.

They will also be required to maintain comprehensive records and report suspicious transactions.

To enforce these requirements, in June 2018 TRACFIN created a dedicated investigation unit which focuses on financial cyber-criminality.

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

All the financial institutions and other designated businesses listed under article L. 561-2 of the MFC (see question 3.1) are required to maintain compliance programmes.

The MFC compels such institutions to:

- assess money-laundering and terrorism-financing risks with regard to the entity's activities;
- put in place internal controls and processes to prevent the risks of money laundering and terrorism financing;
- appoint a Compliance Officer with sufficient knowledge of the risks to which the entity is exposed in terms of money laundering and terrorism financing; and
- take into account the risks in terms of money laundering and terrorism financing in their recruitment policy.

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

Under article D561-31-1 of the MFC which entered into force on October 1, 2013, payment, credit and cryptocurrency institutions must report to TRACFIN, within 30 days after the transaction, any transaction in cash or electronic currency reaching certain thresholds. These thresholds are set out as follows:

- €1,000 per client over one calendar month for transactions in cash; and
- €2,000 per client over one calendar month for transactions in electronic currencies.

In addition, the MFC provides that payment, credit and cryptocurrency institutions must report to TRACFIN cash deposits or withdrawals of an amount exceeding €10,000 per client for one calendar month.

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

All financial institutions and other designated businesses listed under article L. 561-2 of the MFC (see question 3.1) must report to TRACFIN any transaction presenting a high risk of money laundering or terrorism financing with regard to:

- the country or territory of origin or destination of the funds; and
- the nature of the operation in question or the nature of the legal structures involved in these operations.

The MFC also requires such entities to report any suspicious activity (see question 3.9).

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

There is no transaction reporting requirement specifically applicable to cross-border transactions. However, the previously detailed report requirements are applicable to these cross-border transactions.

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

The customer identification and due diligence requirements for financial institutions and other businesses subject to AML requirements may vary depending on the level of risk of money laundering of the activity.

First, they must define and implement identification and evaluation processes for money-laundering risks, including, among other indicators, the specific characteristics of each client. This must lead to a suitable AML policy.

Then, the MFC compels financial institutions and other businesses, before entering into and during a business relationship, to identify their customer and if necessary, the beneficial owner, as well as to gather all information regarding the nature and object of the business relationship.

Nevertheless, there are simplified due diligence requirements when the money-laundering risk is low, or if the customer is listed as a low money-laundering risk operator, where there is no suspicion of money laundering.

On the contrary, the MFC provides additional due diligence requirements when:

- a customer, or when it applies to a beneficial owner, is specifically exposed to specific risks considering his past or present political, judicial or administrative functions or if he has a family member or a person affiliated to him who has such function;
- a transaction, of its own nature, may represent a particular money-laundering risk – for example, when anonymity is preserved; and
- a transaction is, for a personal account or for the account of a third party, established in a country listed by the Financial Action Task Force ("FATF") or by the European Commission as a country obstructing the fight against money laundering.

Finally, when a transaction is complex, is for an unusually high amount, does not have an economic justification or seems to be part of an illegal activity, financial institutions and others businesses must apply a stronger due diligence on such transaction, particularly to know the origin of the funds and their final destination.

Specific dispositions apply for occasional customers and beneficiaries of life insurance transactions.

These aforementioned due diligence requirements are mandatory in order to pursue a business relationship with a customer. If the entity cannot comply with the aforementioned obligations, it must interrupt the business relationship and must not proceed with the transaction.

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

Financial institution accounts for foreign shell banks are prohibited. The prohibition only applies to financial institutions listed in paragraph 1° to 1° *quarter* and 5° to 6° *bis* of article L. 561-2 of the MFC.

### 3.9 What is the criteria for reporting suspicious activity?

Financial institutions must report any transaction or activity registered in their books which they know, suspect or have good reason to suspect are the result of an offence punishable by a jail sentence of more than a year. They must also report any transaction or activity registered in their books which they know, suspect or have good reason to suspect are the result of tax fraud and when at least one criterion listed in article D. 561-32-1 is met.

The Courts have defined what a suspicious activity is. Sums of money resulting from criminal activities are suspect. Likewise, any transaction associated with unusual and complex circumstances or deprived of economic justification must be considered as suspect. If, after attempting to determine the source or destination of the funds, the financial institution still has doubts, the activity should be considered suspicious. Financial institutions must always check the consistency of the controversial amount with the customer's professional activity and his personal assets.

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

As mentioned in question 3.1, the MFC requires all companies registered in France or all foreign companies having a branch, or any legal entity registered in France, to obtain and keep accurate and up-to-date information on their beneficial owners. This information must be communicated to the Trade and Companies Registry.

Eventually, the information collected is gathered in a Registry of Beneficial Owners (created by decree n°2017-1094). Only French authorities such as TRACFIN and persons subject to AML requirements listed under article 561-2 of the MFC (financial institutions, insurance companies, etc.) can have access to this Registry.

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

EU Regulation 2015/847, applicable in France since May 20, 2015, imposes an obligation on payment service providers to ensure that transfers of funds are accompanied by information on the payer, such as name, account number, address or official identity document number, but also on the payee. In the event of difficult identification due to missing information, guidance to assist payment service providers will be issued by the European supervisory authorities.

However, the verification of the accuracy of the information collected by payment service providers should be carried out only for transfers of funds between individuals for any amount above €1,000.

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

Given the anonymity it guarantees, the ownership of legal entities in the form of bearer shares, strictly speaking, is prohibited in France. The only form of ownership similar to bearer shares is called "identifiable bearer securities" and requires the communication of the identity of the owner of the shares, which will be recorded in a register.

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

As stated in question 3.1, apart from financial institutions, some professional occupations are subject to AML requirements, such as gambling and betting operators, art and antiques dealers, accountants, lawyers, notaries, auction sellers and sport agents.

These professionals have:

- a duty of care regarding their clients;
- the obligation to report to TRACFIN any sums entered in their books or transactions involving sums that they know, suspect or have good reason to suspect derive from an offence punishable by a custodial sentence of more than one year; and
- to implement internal controls and processes aimed at preventing money laundering and terrorism financing.

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

Financial institutions listed under article 561-2 of the MFC are under specific anti-laundering requirements when they deal with certain persons or when they operate within certain jurisdictions. They must apply reinforced AML measures when:

- the client (or his beneficial owner), or the beneficiary of a life insurance or capitalisation contract (or his beneficial owner), is a person who is exposed to particular risks by reason of the political, jurisdictional or administrative functions which he exercises or has exercised, or those which are exercised or have been exercised by direct members of his family or persons known to be closely associated with him or have become closely associated with him over the course of a business relationship;
- the proceeds or the operation presents a particular risk of money laundering, in particular when they favour anonymity; and
- the operation is an operation for a personal account or for the account of a third party carried out with a natural or legal person, domiciled, registered or established in a state or territory appearing on the lists published by the FATF among those whose legislation or practices hinder the fight against money laundering and terrorist financing, or by the European Commission pursuant to article 9 of Directive (EU) 2015/849 of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

## 4 General

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

The EU published the 6th AML Directive on November 12, 2018. The Directive must be transposed into the national law of EU Member States by December 3, 2020 and implemented by banks and financial institutions by June 3, 2021. The main measures introduced by the Directive include:

- A harmonised definition of money-laundering offences in the national legislation of EU Member States.
- The clarification of 22 predicate offences for money laundering, including cybercrime and environmental crime.
- The qualification of the offences of "aiding and abetting money laundering" and "self-money laundering" as criminal offences.

**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 its last evaluation by the FATF (February 2011), France's AML framework was found generally satisfactory although some deficiencies were identified, mainly regarding its confiscation and preventive measures for politically exposed persons and sanctions regime for designated non-financial businesses and professionals (such as real estate agents and lawyers). Since the evaluation, France has revised its AML regulations and transposed the 4th and 5th EU AML Directives. The next round of evaluation by the FATF is scheduled for 2020–2021.

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

France was last evaluated by the FATF during 2010–2011. The Report was published in February 2011 and is available at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20France%20ful.pdf (in French).

**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 laws and regulation can be found in French on the website https://www.legifrance.gouv.fr/. The following codes are translated in English: the Criminal Code; Criminal Procedure Code; and MFC.

The AMF and the ACPR also provide guidelines in English on their respective websites.

**Alexis Gublin**, founding partner, has been practising criminal defence in complex transnational litigation matters, particularly in the industrial, defence and energy sectors, for more than 25 years. Alexis represents companies and individuals in cross-border litigation and investigations at all stages of the proceedings. He has extensive experience in the area of criminal defence and has been involved in a wide range of criminal cases before numerous courts, both in France and abroad. Alexis provides advice and representation in a broad range of subjects including anti-money laundering, anti-corruption and tax fraud, and is renowned for being one of Paris' leading white-collar criminal defence attorneys. Alumnus of the Institute of Advanced Studies in National Defence, he lectures at the French National School for the Judiciary, the Parisian Bar School, the Institute of Advanced Studies in National Defence, the National Institute of Advanced Studies in Security and Justice and the Military School.

**Delecroix-Gublin**
11 rue Roquépine
75008 Paris
France

Tel: +33 1 4544 9868
Email: gublin@delecroix-gublin.com
URL: www.delecroix-gublin.com

**Pierre Calderan** joined the firm in 2016. He is admitted to the Paris and New York Bars. Pierre focuses his practice on white-collar criminal defence, international criminal law and military criminal law. He also represents and assists clients in relation to compliance matters and internal investigations. Before joining the firm, Pierre previously worked for a hedge fund management company in Paris. He completed parts of his studies in the United States and in Scotland.

**Delecroix-Gublin**
11 rue Roquépine
75008 Paris
France

Tel: +33 1 4544 9868
Email: calderan@delecroix-gublin.com
URL: www.delecroix-gublin.com

**Louise Lecaros de Cossio** has been an associate at Delecroix-Gublin since 2019. She is admitted to the Paris and Madrid Bars. Louise focuses her practice on white-collar crime and international law matters, including international criminal law, human rights and arbitration. Prior to joining the firm, Louise worked in a public international law boutique in London and as an associate in the Arbitration and Litigation department of a law firm in Madrid. She has also worked in various international organisations.

**Delecroix-Gublin**
11 rue Roquépine
75008 Paris
France

Tel: +33 1 4544 9868
Email: lecarosdecossio@delecroix-gublin.com
URL: www.delecroix-gublin.com

**Thomas Bourceau** has been an associate at Delecroix-Gublin since 2018 and will be admitted to the Paris Bar in 2020. Thomas focuses his practice on white-collar criminal defence, international criminal law and military criminal law. He also represents and assists clients in relation to compliance matters and internal investigations. Before joining the firm, Thomas previously worked within the legal department of Total and EDF in the fields of international contract law, M&A and corporate law, competition law and compliance. He has also studied in England and India.

**Delecroix-Gublin**
11 rue Roquépine
75008 Paris
France

Tel: +33 1 4544 9868
Email: bourceau@delecroix-gublin.com
URL: www.delecroix-gublin.com

Founded in January 1994, Delecroix-Gublin specialises in white-collar crime and assists its clients in all stages of investigations and proceedings, both in France and abroad.
The firm has earned recognition in the field of criminal defence, particularly for its cutting-edge expertise in anti-corruption and AML and has developed a renowned internal investigations practice.
The firm's team is accustomed to representing large groups operating in a wide variety of sectors such as energy, defence, construction, the oil industry and telecoms.
The firm works in coordination with various international and local law firms in jurisdictions across the globe within the context of cross-border investigations.

The firm's expertise has been recognised by *The Legal 500*, *Décideurs*, and *Who's Who Legal* rankings.

**www.delecroix-gublin.com**

Delecroix Gublin AVOCATS À LA COUR

# Germany


Dr. Dirk Seiler


Enno Appel

Herbert Smith Freehills LLP



## 1 The Crime of Money Laundering and Criminal Enforcement

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

In Germany, money laundering is prosecuted at a regional level by the respective state prosecutors' offices. Investigations are conducted by the State Office of Criminal Investigations (*Landeskriminalamt*) and local police.

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

Criminal money laundering pursuant to Section 261 of the German Criminal Code (StGB) entails the following elements: (1) money or other assets are the proceeds of a predicate offence; (2) the proceeds were intentionally concealed, disguised, procured (for himself or a third party), used (for himself or a third party) 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 by not recognising the criminal origin. In the latter case, the maximum sentence is reduced.

Predicate offences are (attempts to commit the offence suffice):

- severe crimes with a minimum sentence of at least one years' imprisonment (e.g. robbery);
- active and passive bribery of public officials; drug-related offences; commercial, forceful or organised evasion of customs and violation of customs provisions and smuggling/procuring such goods; and
- subversive acts of violence capable of threatening the existence or the security of the state/international institution; formation of criminal/terrorist associations as well as committing of criminal offences as a member of a criminal/terrorist association, if not already a predicate offence.

The following offences qualify as predicate offences only if committed in a continued manner as part of commercial activity or within an organised association:

- tax evasion; forgery of credit cards and cheque cards; pimping; human trafficking; exploitation of another person through labour (e.g. slavery); theft, concealment, extortion; receiving stolen goods; fraud and specific types of it; embezzlement; forgery of documents and related offences, unauthorised organisation of gaming; unauthorised dealing with toxic waste, or radioactive or other hazardous substances; commercial active and passive bribery; illegal smuggling of foreigners; inciting improper applications for asylum; insider trading; and offences related to intellectual property, e.g. copyright infringement.

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

In general, German criminal law is applicable if the crime was committed in Germany (Sections 3, 9 StGB) or on an aircraft/ship operating under the German flag (Sections 4, 9 StGB). This includes every place where the offender acted or in which the result – if it is an element of the offence – occurs.

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

Money laundering of the proceeds of foreign crimes is punishable in Germany if the predicate offence is also punishable in the foreign country (Section 261 (8) No 8 StGB).

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

Regional state prosecutors are responsible for investigating and prosecuting money laundering criminal offences. (See question 1.1 above.)

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

German criminal law only applies to natural persons. However, there are provisions in the Administrative Offences Act (OWiG) imposing fines upon companies if criminal offences have been committed by executive employees, and/or if the executive employees have failed to adhere to their supervisory obligations relating to the prevention of criminal offences (Sections 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 and begins after the offence has ended.

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

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

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

Sections 73 *et seq.* StGB apply to all criminal offences including money laundering/predicate offences. It is the court in the relevant district which issues the confiscation order.

Subject to confiscation are assets which have been obtained by or used for the criminal offence, i.e. proceeds of crime (Section 73 StGB), instrumentalities of the crime 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.
- "Indirect Proceeds", i.e. benefits derived from 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 be 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 at the time of the court order.

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 that the assets are proceeds of a crime or if the offender acted for them (Section 73b/74a StGB).

The court may also order that the value of the obtained assets will be confiscated if confiscation of the actual asset is not possible (Section 73c StGB).

Assets of a company can be confiscated if the crimes were committed by its representative bodies or legal representatives (Section 74e StGB).

In general, confiscation can only be ordered on the basis of a conviction. There are, however, exceptions to this rule:

- Proceeds, instrumentalities and objects can be confiscated if no one can be convicted and prosecuted for the crime (Section 76a StGB).
- There are provisional measures in German civil law which allow for the provisional seizure of assets, but only for the purpose of ensuring that they are not divested of until the underlying dispute has been resolved and to secure a later enforcement (Sections 916 *et seq.*).

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

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

In 2019, prosecutors initiated investigations against employees of a Bank concerning alleged aiding and abetting of money laundering in connection with the Danske Bank scandal.

Other investigations against employees of a German Bank concerning alleged aiding and abetting of money laundering which were initiated by Frankfurt prosecutors in 2018 were dropped for lack of probable cause in 2019. However, the bank paid EUR 15 million to the state prosecutor's office.

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 a German Bank for money laundering in a continued manner as part of commercial activity and within an organised association. The employees allegedly helped to channel approx. USD 113 million from Russia through Europe and Bermuda.

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

Section 153 German Code of Criminal Procedure (StPO) stipulates that prosecution may be ceased if the crime is minor and if the public does not have any interest in prosecution. The cease decision may be combined with an order to pay a fine. The cease decision is not public.

There is the possibility to enter into a deal during court proceedings if all participants agree and only with respect to the extent of the sentence (Section 257c StPO). The details of the deal are not public.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

The supervising and monitoring authorities are for:

- banks and other financial institutions: Federal Financial Supervisory Authority (BaFin);
- lawyers and legal advisors: local bar/professional associations;
- notaries: president of the regional court in the relevant district;
- auditors, registered accountants and tax advisors/agents: chamber of the profession, for example, the Chamber of Tax Advisors; and
- casinos, gaming companies and commercial traders of goods (*Güterhändler*): the respective supervisory authority of the federal states.

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

Lawyers, legal advisors, notaries, auditors, registered accountants and tax advisors/agents are regulated by local self-regulatory bodies. These 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 local self-regulated bodies are responsible for compliance and enforcement.

**2.4 Are there requirements only at national level?**

The money laundering requirements are entirely codified in the federal Anti-Money Laundering Act (GWG) and partially in the Banking Act (KWG).

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

The German regulator BaFin has published interpretative and application notes (*Auslegungs- und Anwendungshinweise*) for the implementation of the due diligence and internal safeguard measures to prevent money laundering. See also question 2.1 above.

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

The FIU (*Zentralstelle für Finanztransaktionsuntersuchungen*) has been established at the General Directorate of Customs (*Generalzolldirektion*). The FIU's core responsibility is to analyse and assess filed suspicious activity reports. In this regard, it also has unlimited access to data of prosecution offices, public financial agencies and public administrative agencies. Furthermore, it has the power to halt suspicious transactions for up to one month. The FIU will decide whether the case needs to be forwarded to the prosecution offices. The FIU also coordinates international collaboration with foreign authorities.

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

The limitation period for prosecuting money laundering-related administrative offences is three years (Section 31 OWiG).

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

Section 56 (2), (3) GWG set out that for particularly grave and systematic offences and for specific obliged entities the maximum fine is between EUR 1 to 5 million or 10 per cent of the gross income of the entity in the preceding year, depending on which figure is higher. In all other cases, a fine of up to EUR 100,000 may be imposed.

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

Depending on the gravity of the offence, it is possible that the responsible authority revokes required licences on account of permanent violations of anti-money laundering provisions (e.g. Section 35 (2) No 6 KWG and Section 51 (5) GWG).

Furthermore, for financial institutions BaFin may demand the dismissal of the managers responsible and may also prohibit these managers from carrying out their activities at institutions organised in the form of a legal person (Section 36 (1) and (2) KWG).

The competent authority has the power to order specific 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.

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. Sections 44 *et seq.* KWG).

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

In principle, the penalties described above (see question 2.8 above) are administrative in nature. In addition to 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).

**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, and brokers; gambling companies; and companies which commercially trade goods.

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

As of 1 January 2020, crypto custody business has been incorporated into the KWG as a new financial service and is thus explicitly regulated by law. Anti-money laundering requirements apply to all financial services entities offering crypto custody businesses.

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

All obliged entities are required to implement procedures comprising, *inter alia*, an efficient risk management system which sufficiently ensures that the due diligence, reporting and record-keeping obligations are met and regularly monitored and that necessary suspicious activity reports are filed.

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

General due diligence obligations are triggered by the establishment of a business relationship or 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. For example, for gambling companies the threshold is EUR 2,000, for companies commercially trading goods if they accept cash of EUR 10,000 and above, and for insurance agents if they receive more than EUR 15,000 in cash within a year.

Meeting these thresholds does, however, not necessarily mean that the reporting obligation in Section 43 GWG is triggered. The reporting obligation does not specify the value of a transaction as a triggering factor. The provision vaguely refers to circumstances which appear suspicious.

Financial institutions have the specific obligation to retain records regarding large and complex transactions which is part of their customer due diligence obligation, and which they must do regardless of the client's risk qualification. The records must sufficiently demonstrate that the obligation was complied with (Section 25 h (3) KWG).

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

No, there are no such requirements other than in cross-border transactions (see question 3.6).

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

For cross-border transactions, the Foreign Trade and Payments Act (AWG) in conjunction with the Foreign and Trade and Payments Regulation (AWV) applies, which entails reporting obligations which have to be filed electronically to the Federal Bank of Germany (*Bundesbank*) subject to certain deadlines. The Federal Bank may issue exemptions to these obligations on a case-by-case basis.

Payments exceeding EUR 12,500 must be reported (Section 67 AWV): all residents in Germany including companies will have to report to the Federal Bank if they receive or make payments exceeding EUR 12,500 (or the equivalent in foreign currency) from a non-German resident or from a German resident, but for the account of a non-German resident (incoming and outgoing payments). The obligation does not apply to cash physically carried abroad. The Federal Bank provides the relevant forms for the reporting. The term 'resident' does not refer to nationality but rather the place of habitual residence, which means that if a German citizen has been living abroad for more than one year he will be considered a non-resident. There

are exemptions to this, *inter alia*, payments received/made for exported/imported goods, payments and repayments of loans and deposits with an original maturity of up to 12 months, and payments made by financial institutions within long-term credit transactions with non-residents.

Resident banks and similar financial service entities have an additional obligation with respect to payments exceeding EUR 12,500 if those relate to the sale of stocks, derivatives to/from foreigners or encashing of such, payment of interest and dividends on resident stocks to/from foreigners, or payments related to interests (Section 70 AWV).

Other reporting obligations relate to assets exceeding a certain value if held by a resident abroad and such assets held by a non-resident in Germany (Section 65 AWV), claims and debts relating to funds of resident financial institutions exceeding EUR 5 million, investment stock companies and capital management companies (Section 66 AWV) and claims and debts exceeding EUR 500 million resulting from financial relationships with foreigners of the same entities (Section 66 AWV). A violation of these provisions may result in an administrative fine (Section 81 AWV).

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

General due diligence obligations have to be performed regardless of the risk classification and are triggered when a business relationship is established and for one-off transactions exceeding the thresholds (EUR 1,000 in very specific cases and usually EUR 15,000) and if there are suspicious indications.

The obligations are: (1) identification of the client by obtaining the information specified in Section 11 GWG and verification of this information through, *inter alia*, documents specified in Section 12 GWG; (2) identification and verification of the person acting on behalf of the client; (3) clarification of whether the client acts for a beneficial owner and if so, identification of the beneficial owner and verification of the obtained information; and (4) obligations to conduct a risk analysis and implement a risk management system including business and customer related internal safeguards such as, e.g. internal policies, the appointment of an anti-money laundering officer, etc.

When assessing the customer-related risk, the entities must at least consider the purpose of the business relationship, the amount of the assets and the regularity and duration of the business relationship.

Relationships with high-risk clients additionally trigger enhanced due diligence obligations, *inter alia*, obtaining information on the source of wealth, enhanced monitoring and obtaining management approval. A high risk exists if one of the following applies: the client or beneficial owner is a politically exposed person, a family member or closely related person; or a transaction is unusual with respect to complexity, size or is conducted for no economic or rightful purpose (Section 15 (3)). Annex 2 of the GWG contains additional high-risk indicators.

Correspondent relationships between financial institutions and comparable financial entities located in a third-party state are considered and will trigger obligations specific to correspondent relationships (Section 15 (6) GWG).

If the client is categorised low risk, the entity is, *inter alia*, allowed to reduce the intensity of the measures. They may, in particular, deviate from the specific verification requirements. Annex 1 contains specific low-risk indications in a non-exhaustive list (Section 14 GWG).

Parent companies which have subsidiaries abroad are required to ensure that such processes and safeguards exist throughout their group (Section 9 GWG).

For financial institutions, the described obligations apply and are supplemented by the KWG which contains more specific requirements with respect to, e.g. required internal safeguards (Sections 25 *et seq.* KWG).

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

For credit institutions, business relationships with shell banks are prohibited pursuant to Section 25m KWG.

**3.9 What is the criteria for reporting suspicious activity?**

Pursuant to Section 43 GWG, a report has to be filed without undue delay if the facts indicate that the assets which are connected to the business relationship, a specific transaction, or a brokerage relates to a crime which is a predicate offence to money laundering, to terrorist financing, or if there are indications that the client failed to disclose beneficial ownership.

Lawyers, notaries, patent lawyers, auditors, tax advisors and similar professions might be exempted from suspicious activity reporting if the respective circumstances are covered by their professional privilege.

According to Section 261 (9) StGB, an offender is exempt from any penalty if he or she either reports the crime voluntarily to the responsible authority or ensures seizure of the respective assets. The suspicious activity report may qualify as such a voluntary report and may, thus, exclude a criminal penalty.

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

In 2017, Germany established a "Transparency Registry" and legal entities, shareholders and trustees are required to disclose information on their beneficial ownership to the responsible authority.

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

Payment orders are required to include sufficient information about the originator (name or customer ID) and an account number to which the transfer is made. However, the bank is not required to check whether the name on the payment order matches the account number.

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

Yes, it is permitted; however, it will be deemed a risk-enhancing factor.

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

The GWG provisions apply to a variety of non-financial institutions.

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

The GWG also applies to persons commercially trading with goods (see question 3.1 above), but there are no specific anti-money laundering requirements for free trade zones.

## 4 General

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

There are ongoing discussions in Germany as to whether there is a need for corporate criminal liability. The first draft of the new law was published in April 2020.

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

It has been pointed out in the 3rd Follow-up Report of the FATF in 2014 that Germany lacks criminal liability for self-laundering. Recommendations that had been made in the previous report, such as an incomplete list of predicate offences, were addressed by the German legislator, according to the FATF.

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

Yes, see question 4.2. The report is titled "Mutual Evaluation of Germany: 3rd Follow-up Report" and can be accessed through the following link: http://www.fatf-gafi.org/media/fatf/documents/rep orts/mer/FUR-Germany-2014.pdf.

The next evaluation is scheduled for 2020.

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

The most relevant texts are available on the website of BaFin. For example, you can find an English translation of the GWG here: https://www.bafin.de/EN/RechtRegelungen/Rechtsgrundlagen/Gesetze/gesetze_artikel_en.html?nn=8356586.

**Dr. Dirk Seiler** is a partner in the Dispute Resolution/Corporate Crime and Investigations practice group at our Frankfurt office. Dirk has been advising 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, fraud and anti-money laundering. He has been a certified specialist in criminal law (*Fachanwalt für Strafrecht*) since 2007. In the area of preventive compliance consultancy, Dirk has been representing a number of high-profile companies from various sectors for many years.
Dirk is a regularly recommended lawyer in the leading German Law directories for Compliance, Investigations and White Collar Crime advice.

**Herbert Smith Freehills LLP**
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Tel: +49 69 2222 82535
Email: dirk.seiler@hsf.com
URL: www.herbertsmithfreehills.com

**Enno Appel** is a senior associate in our Dispute Resolution/Corporate Crime and Investigations practice group at our Frankfurt office. He specialises in advising and representing national and international companies in the fields of compliance/white-collar crime and the associated internal investigations and lawsuits. Enno regularly advises international banks and other clients on regulatory obligations under the anti-money laundering (AML) and anti-bribery and corruption (ABC) laws and in cases of fraud and embezzlement. Enno has been recognised as one of the next generation's lawyers in the area of Internal Investigations.

**Herbert Smith Freehills LLP**
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Tel: +49 69 2222 82516
Email: enno.appel@hsf.com
URL: www.herbertsmithfreehills.com

Our lawyers in Düsseldorf and Frankfurt provide local and international clients with leading expertise in dispute resolution, competition/regulatory, corporate/M&A, finance, capital markets, real estate and employment matters, general commercial issues as well as advice on compliance matters, corporate crimes and investigations.
With a major focus on cross-border work we operate seamlessly within our global network to provide clients with the highest level of service. Through continuous effort the German practice has grown significantly over the past years.

**www.herbertsmithfreehills.com**

# Greece

Anagnostopoulos


Ilias G. Anagnostopoulos


Alexandros D. Tsagkalidis

## 1 The Crime of Money Laundering and Criminal Enforcement

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

Criminal law enforcement lies with the Prosecutor's Office. All enforcement agencies (the Hellenic FIU, the Financial and Economic Crime Unit, the Capital Market Commission, etc.) forward their reports with findings and gathered information of suspicious activities to the Prosecutor's Office. As a general rule, enforcement agencies have the power to collect information, report their findings and proceed with necessary investigative acts. However, everything is coordinated by the prosecutor. The prosecutor evaluates the material in hand and initiates whatever proceedings are necessary.

In cases of emergency, certain powers are given to the Hellenic FIU for securing traced assets (proceeds of crime or related to money-laundering activities) whereby the head of the Hellenic FIU issues a freezing order in order to prevent loss or further concealment of property. These orders are also reviewed by the prosecutor and, if necessary, following a request by the interested party, by a judicial council.

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

Law 4557/2018 is the main law against money laundering. According to article 2, the act of money laundering is described as follows:

- knowingly converting and transferring property assets that are the proceeds of a crime, or participation in such an act for the purposes of concealing the illegal sources of the assets, or aiding anyone involved in said acts in order to assist in avoiding legal sanctions;
- concealing and covering up the truth, by any means, in relation to the source, movement, disposal, place of acquiring assets or asset-related rights, knowledge that a property is associated with the proceeds of criminal acts or participation in criminal activities;
- acquiring, possessing, managing or using any asset with the knowledge that at the time of possession, management, etc., such property asset was the proceeds of a criminal activity;
- using the financial sector by depositing or transferring proceeds of criminal activities for the purposes of making it appear as though they have legitimate sources;
- forming a group or organisation for the purposes of committing one or more of the above-mentioned actions; and
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in the above points.

Furthermore, it is required that the natural person acts in the knowledge (*dolus directus*) of the source of the assets and for the purposes of concealing or covering up their true origin. Therefore, there is no room for negligently committing an act of money laundering.

Article 4 of Law 4557/2018 contains a list of predicate offences of money laundering. The list contains all forms of classic corruption and property-related offences, namely, bribing of domestic public officials, bribing of foreign officials or EU officials, fraud, tax evasion and tax fraud, capital market offences, including offences related to insider trading, antiquities trafficking, environmental offences, drug trafficking, people trafficking, organised crime and terrorism financing. Tax evasion is listed as a predicate offence as well.

Moreover, the list contains a general provision according to which any offence that results in asset or property profits and is punishable by law with a minimum of six months' imprisonment may be considered a predicate offence. In other words, all criminal activities that can produce money or asset gains or profits may be considered as predicate offences. This provision makes the list of predicate offences non-exhaustive, since it leaves room for any type of criminal behaviour that results in profit, even if it is of lesser to medium importance (as it includes misdemeanours punishable by imprisonment of a few months).

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

In principle, AML legislation and regulations apply to individuals and institutions based in Greece or that are active within the Greek territory. Greek money-laundering laws are applicable to Greek citizens and non-citizens even if the predicate offence has been committed abroad, as long as it constitutes an offence in accordance with the laws of the foreign country and provided that the laundering act was committed within Greek territory. Moreover, Greek citizens may be prosecuted for laundering acts committed in a foreign country, provided that the dual criminality requirement is fulfilled.

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

Please see the answer to question 1.1.

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

Criminal liability lies with a natural person, and consequently there is no criminal liability in its traditional sense regarding a business or entity. For the purposes of applying legal provisions related to corporate practices and activities, there are provisions for liability in the form of administrative penalties and fines, depending on the seriousness of the act, size of the business, etc.

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

The maximum penalties are as follows:

Individuals: Incarceration of up to 15 years and a monetary sentence of up to €2 million.

Legal entities: An administrative fine ranging from €50,000 up to €10 million, which is always applicable, and:

i) suspension of activities temporarily or permanently;
ii) prohibition of certain activities to be performed by the company, or establishment of branches; and
iii) a ban from public tenders, subsidies, etc.

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

The statute of limitations is 15 years from the time the offence was committed. This period is suspended for five years when the case file is forwarded to a trial hearing.

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

No, there are no parallel state or provincial criminal offences.

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

Agencies such as the SDOE and the FIU, along with the judicial authorities (the investigating judge and the prosecutor during the main investigation, or the judicial council during the preliminary inquiry), are responsible for tracing and freezing assets that are allegedly the proceeds of crime. Confiscation of such assets can solely be ordered by the court that tries the case if the defendant is found guilty of committing such crimes.

Assets derived from a predicate offence or from money laundering or acquired directly or indirectly from the proceeds of such offences, or the means that were used or were going to be used for committing these offences, shall be seized. According to the provisions found in the new GCCP (e.g. articles 304, 311 par. 3 3 and 373 par. 3), frozen assets shall be used to satisfy the pecuniary damage, which the victim of the crime suffered.

Confiscation shall be imposed even if the assets or means belong to a third person, provided that such person was aware of the predicate offence or the offences referred to in article 2 of Law 4557/2018 at the time of their acquisition. Where the assets or proceeds above no longer exist or have not been found or cannot be seized, assets of a value equal to those assets or proceeds as at the time of the court's judgment shall be seized and confiscated. Their value shall be determined by the court. The court may also impose a pecuniary penalty up to the value of those assets or proceeds if it rules that there are no additional assets to be confiscated or the existing assets fall short of the value of those assets or proceeds.

Furthermore, according to the recently amended article 76 of the Greek Criminal Code, in case of a guilty verdict, all assets derived from the commission of a felony or from a serious misdemeanour, as well as all assets acquired (directly or indirectly) from the proceeds of such offences, are subject to confiscation. In case these assets have been 'mixed' with lawfully obtained assets, confiscation shall apply to assets up to the value of the assets that derived from the offence. Confiscation of assets is not enforced when it is deemed disproportionate (i.e., it is highly likely that it will cause serious and irreparable damage to the defendant's livelihood or to his family).

Moreover, proceeds of crime may be subject to confiscation even when criminal proceedings have not been initiated or have been terminated because of the death, unavailability, etc., of the offender, or if the prosecution was terminated or declared inadmissible on other grounds. In these cases, confiscation shall be ordered by the judicial council or by the court (article 40(3) of Law No. 4557/2018). These decisions are subject to appeal on the merits and on points of law according to articles 495 and 504(3) of the GCCP. Owing to the punitive nature of forfeiture in criminal proceedings, non-conviction-based forfeiture has been said to be in breach of articles 2(1), 7(1) and 96(1) of the Greek Constitution, which establish the principles of *nulla poena sine processu* and *nullum crimen, nulla poena sine culpa*.

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

Financial institutions have been subject to administrative sanctions; appeals against such sanctions are pending before the administrative courts.

Charges against individuals are currently pending before criminal courts.

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

The Greek Criminal Procedure Code does not provide for extra-judicial settlement of criminal actions. Full compensation of the victim for financial losses, etc., may be the basis for leniency or (at an early stage of the proceedings) for the termination of criminal proceedings.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

Enforcement and supervision of covered institutions and persons is done through government entities and quasi-governmental entities which are competent in their respective field. Banking, financial and insurance institutions are supervised by the Bank of Greece. Corporations listed in the stock market are regulated by the Hellenic Capital Market Commission. Other businesses are regulated by the competent department of the relevant ministry (e.g. Ministry of Commerce), lawyers and notaries by the Ministry of Justice, etc. (a comprehensive list is provided for in article 6 of Law 4557/2018). All regulatory agencies and institutions liaise with the central regulating authority, which is the Ministry of Finance.

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

For each category of covered institution, anti-money laundering regulations and guidelines are issued by the supervising administrative authorities (e.g. decisions issued by the Bank of Greece).

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

Yes, they have powers to impose sanctions of an administrative nature.

**2.4 Are there requirements only at national level?**

Greece is a member of the Financial Action Task Force (FATF), the FIU-Net and the Egmont Group through the Hellenic FIU. It is also a member of the EU and the Council of Europe and cooperates with all major international bodies and organisations related to combatting money laundering. In this context, international money-laundering standards and requirements are implemented at a national level.

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

Please see the answers to questions 2.1 and 2.2.

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

The Hellenic FIU is the competent authority to: collect information from reports filed on suspicious transactions or any other source; make use of information communicated by foreign authorities; release guidelines to natural persons or businesses covered by Law 4557/2018 on applying the law; and cooperate and exchange information with international organisations with similar powers. The Hellenic FIU is a member of the FIU-Net and the Egmont Group and files its annual report with the Commission on Transparency of the Hellenic Parliament, the Ministry of Finance, the Ministry of Justice and the Ministry of Citizen Protection.

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

Limitation periods vary depending on the classification of the act as a 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 15 years), the limitation period is 15 years between the act and indictment. After indictment the limitation is suspended for an additional five years.

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

All covered institutions and their employees have three basic obligations (articles 22 and 27 of Law 4557/2018): to report immediately to the FIU on suspecting that an act of money laundering has been committed or is about to be committed; to offer immediately all information requested by the FIU or other supervising authorities; and not to inform the client or any third party either that they have filed a report of suspicious transactions or that they have received a request to give information to any authority. Breach of the latter prohibition is punishable by imprisonment for three months (minimum) to five years and a fine.

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

As per the provisions of article 46 of Law 4557/2018, failure to comply with anti-money laundering regulations may also lead to:

- removal of the directors, the managing director, management officers of the legal entity or other employees for a specific time period and prohibition of assuming other important duties;
- prohibition from carrying out certain activities, establishing new branches in Greece or abroad or increasing its share capital; and
- in case of serious and/or repeated violations, final or provisional withdrawal or suspension of authorisation of the corporation for a specific time period or prohibition to carry out its business.

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

Penalties for breaching anti-money laundering obligations are mainly administrative (please see the answer to question 2.9).

Breach of confidentiality with regard to the reporting of suspicious transactions is punishable by imprisonment for three months (minimum) to five years and a fine (article 27 of Law 4557/2018).

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

In most cases, the supervising authorities are notified by the prosecutorial and police authorities. However, no sanction shall be imposed without prior summons of the legal representatives of the legal entity to provide their views. The summons shall be served 10 working days before the day of the hearing at the latest. The administrative decisions imposing penalties on legal entities may be challenged before the competent administrative courts.

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

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

As per article 5 of Law 4557/2018, the following legal/natural persons are subject to anti-money laundering requirements: a) credit institutions; b) financial institutions; c) venture capital companies; d) companies providing business capital; e) chartered accountants, audit firms, independent accountants and private auditors; f) tax consultants and tax consulting firms; g) real estate agents and related firms; h) casino enterprises and casinos operating on ships flying the Greek flag, as well as public or private sector enterprises, organisations and other bodies that organise and/or conduct gambling and related agencies and agents; i) auction houses; j) dealers in high-value goods, only to the extent that payments are made in cash in an amount of €10,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked; k) auctioneers; l) pawnbrokers; m) notaries and lawyers, when they participate, whether by acting on behalf of and for their clients in any financial or real estate transaction, or by assisting in the planning and execution of transactions for the client concerning the i) buying and selling of real property or business entities, ii) managing of client money, securities or other assets, iii) opening or management of bank, savings or securities accounts, iv) organisation of contributions necessary for the creation, operation or management of companies, or v) creation, operation or management of trusts, companies or similar structures; and n) natural or legal persons providing services to companies and trusts (trust and company service providers) which by way of business provide any of the following services to third parties:

- forming companies or other legal persons;
- acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons or arrangements;
- providing a registered office, business address, correspondence or administrative address and any other related services for a company, a partnership or any other legal person or arrangement;
- acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement; or
- acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market.

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

As per article 3 of Law 4557/2018, electronic and digital assets are considered "property" for the purposes of the said law. Therefore, anti-money laundering legislation is applicable for all transactions involving cryptocurrency.

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

All covered institutions and persons need to implement AML compliance programmes, usually following guidelines and regulations of the competent supervising authorities. Naturally, covered institutions, which are more vulnerable to money-laundering activities (e.g., banks, financial institutions, insurance institutions), have more comprehensive and detailed AML compliance programmes, especially because these institutions are under strict supervision and regulation. The minimum elements of an AML compliance programme (minimum may vary depending on the nature of the covered institution or person) are related to validating the transaction as much as possible and identifying transacting parties in order to eliminate suspicions of questionable conduct or unknown, untraceable origins of assets.

However, even natural persons (e.g., lawyers and notaries) have to meet the standards set by the competent supervising authority (Ministry of Justice, bar associations and notary associations) in relation to the management of trusts or transactions on behalf of the client.

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

Suspicious activity is that which indicates that a money-laundering offence has been committed or attempted, or where there is sufficient indication that the transacting party is involved in other criminal activity (predicate offences). This assessment is made in view of the characteristics of the transaction, the background of the client (financial, professional, etc.) and a history of the client's transactions. Diligence rules apply to transactions over €15,000. Suspicious transactions must be reported immediately to the Hellenic FIU along with all relevant information to be requested by the FIU.

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

The Ministry of Finance has issued a series of circulars in respect of the application of anti-money laundering laws and regulations and bookkeeping obligations, whereby auditors and

accountants are given specific guidelines to report any transaction that causes any suspicion of being related to a criminal act (even if it is a simple or general suspicion without need for proof) to the Hellenic FIU.

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

Cross-border transactions which take place within covered institutions (e.g. money remittances to or from bank institutions in Greece) are subject to the same anti-money laundering requirements as local transactions.

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

Law 4557/2018 outlines a complex set of diligence rules for the covered persons to follow, applicable to new clients, existing clients, high-risk individuals, politically exposed persons, transactions on new financial products, transactions executed without the client's physical presence, etc.

Rules of diligence apply when the covered institutions enter a business agreement with the client, when they process occasional transactions of more than €15,000, when there is suspicion that an offence has been committed or is about to be committed and when there is doubt about the accuracy of information obtained for the purposes of confirming and verifying the identity of the client or another person acting on behalf of the client.

According to the rules of ordinary diligence, covered institutions must take the necessary action to verify the identity of the client and the identity of the beneficial owner in relation to the executed transaction, and to gather information on the economic background of the client in order to check whether a transaction is in accordance with this background, etc.

The means that a financial institution uses to make the necessary cross-references must be appropriate (according to the Law's description) in order to identify the individuals, the transaction and the beneficiary owner.

As regards the beneficiary ownership, there is a description given by the Law (article 4, paragraph 16) and is generally the person in favour of whom the transaction is executed or the person in control of an entity or a group of entities (directly or indirectly) in favour of which the transaction is executed. The main purpose 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 to organised crime and terrorism activities.

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

Yes. Article 17 of Law 4557/2018 stipulates that credit institutions are prohibited from entering into or continuing a correspondent banking relationship with a shell bank and shall not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

**3.9 What is the criteria for reporting suspicious activity?**

Please see the answers to questions 3.4 and 3.5. It should be noted that confirmation and verification of the identity of the customer and the beneficial owner shall take place prior to the conclusion of the business relationship or the execution of the transaction. Such verification of the identity may be completed during the establishment of a business relationship, if necessary, so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such cases, said verification procedures are completed as soon as possible after the initial contact. Moreover, the opening of an account with a credit institution or financial institution shall be allowed even before full compliance with customer due diligence requirements is ensured, provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf. In the case of life insurance, verification of the identity of the policy beneficiaries identified or designated shall be made at the time of payout. Casinos operating on ships in Greece or flying the Greek flag are required to verify the identity of their customers upon their entry into the gambling venue. If they keep records of earnings payments and nominal redemption of chips, those shall be kept for at least five years and shall be available to audits.

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

Yes, through the General Electronic Commercial Registry (GEMI) which keeps information on all legal forms of businesses in Greece.

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

Yes, it is.

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

Ownership of legal entities in the form of bearer shares is permitted. However, for certain types of legal entities (such as

banking institutions, telecommunications companies, etc.), the law provides that ownership is permitted solely in the form of registered shares.

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

Such requirements are established in decisions issued by the competent Ministries.

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

Yes; for instance, Law 4557/2018 has specific provisions regulating the operations of casinos.

## 4 General

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

Please refer to sections 2 and 3 above.

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

Following Law 4557/2018, which transposed Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Greece's anti-money laundering efforts and tactics are in line with most European and international standards.

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

The FATF performed an on-site visit to Greece between 30 October to 16 November 2018. Its report was published on 3 September 2019 and analysed the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Greece's AML/CFT system. As regards the overall level of compliance and effectiveness, FATF noted that Greece has implemented an AML/CFT system that is effective in several areas. A substantial level of effectiveness has been achieved in the areas of understanding the ML/TF risks and the national co-ordination, collection and use of financial intelligence, investigation and prosecution of terrorist financing and the implementation of targeted financial sanctions related to proliferation. In terms of technical compliance, the legal framework is particularly strong, with only some areas in need of significant improvement: measures related to preventing misuse of legal structures and the non-profit sector, correspondent banking and cash couriers.

**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 G. Anagnostopoulos** has advised and represented corporates and individuals in prominent cases in multiple jurisdictions over the past three decades. His practice focuses on complex matters involving financial fraud, corrupt and anti-competitive practices, tax and money-laundering offences, extradition and mutual assistance requests. He regularly offers his opinion, as a legal expert, in domestic and foreign jurisdictions.

Since 2013, Ilias has chaired the Hellenic Criminal Bar Association, and from 2006 to 2013 he chaired the criminal law committee of the Council of the Bars and Law Societies of Europe (CCBE). He is a professor in criminal law and criminal procedure at the School of Law, National and Kapodistrian University of Athens. Ilias 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.

**Anagnostopoulos**
6, Patriarchou Ioakeim
106 74, Athens
Greece

Tel: +30 210 729 2010
Email: ianagnostopoulos@iag.gr
URL: www.iag.gr

**Alexandros D. Tsagkalidis** has been with Anagnostopoulos since 2008. He has advised and represented high-end clients in complex white-collar crime cases with trans-jurisdictional aspects and has gained broad experience in business crime, corruption and anti-competitive practices, money laundering, asset recovery, financial fraud, tax offences, extradition and mutual assistance requests. He is a member of the Legal Experts Advisory Panel of Fair Trials International. Alexandros has published in Greek and English on matters of business crime, investigation procedures, money laundering, European criminal law, defence rights, extradition and surrender procedures.

**Anagnostopoulos**
6, Patriarchou Ioakeim
106 74, Athens
Greece

Tel: +30 210 729 2010
Email: atsagkalidis@iag.gr
URL: www.iag.gr

Anagnostopoulos is a leading Athens-based practice established in 1986 that assists corporates and select individuals in managing criminal and regulatory risks. The firm is noted for combining sophisticated advice with forceful litigation in a wide variety of practice areas, and over the years has built a reputation as a high-end team of specialists who take a holistic and creative approach to complex cases and are fully committed to their clients' needs, while upholding high standards of ethics and professional integrity. The firm responds to the emerging needs of corporate clients in respect to specific aspects of corporate governance and liability, drawing upon a solid knowledge base in corporate criminal liability, internal company investigations and compliance procedures, corruption practices and cartel offences. The firm's litigation group is led by Ilias G. Anagnostopoulos, who is considered one of the foremost white-collar crime experts, and the firm is distinguished by its track record in high-profile cases.

**www.iag.gr**

# Indonesia



Ardian Deny Sidharta


Oene J. Marseille


Erie H. Tobing


Aris Budi Prasetiyo

Soemadipradja & Taher




## 1 The Crime of Money Laundering and Criminal Enforcement

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

There are two government bodies that are authorised to prosecute money laundering and predicate offences in Indonesia, namely the Attorney General of the Republic of Indonesia ("**AG**"), which prosecutes money laundering and predicate offence case files assigned by an investigator, and the Corruption Eradication Commission ("**KPK**"), which prosecutes money offences and predicate offence case files assigned by a KPK investigator.

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

To establish money laundering as a criminal offence, prosecutors and investigators must be able to prove the elements of offences set out under Articles 3, 4, or 5 of Law No.8 of 2010 ("**Law 8/2010**"), namely:

- any person who places, transfers, assigns, spends, pays, grants, deposits, takes overseas, changes the form of, exchanges with the currency or securities or other deeds over Assets which are recognised or which are reasonably suspected as being the result of a crime, as set forth in Article 2(1) in order to hide or to disguise the origin of the Assets (Article 3);
- any person who hides or disguises the origin, source, location, purpose, transfer of right or the true ownership of Assets that are known by him or of which are reasonably suspected as being the result of a crime, as set forth in Article 2(1) (Article 4); or
- any person who accepts or who takes control of the placement, transfer, payment, grant, deposit, exchange of, or utilises Assets which are known by him or which are reasonably alleged as being the result of a crime, as set forth in Article 2(1) (Article 5(1)).

Article 2(1) of Law 8/2010 states that the proceeds of money-laundering offences shall be any assets obtained from predicate offences, including:

- corruption;
- bribery;
- narcotics;
- worker or immigrant smuggling;
- crimes related to banking;
- crimes related to the capital market;
- crimes related to insurance;
- human trafficking;
- illegal firearms trade;
- terrorism;
- burglary;
- embezzlement;
- fraud;
- money counterfeiting;
- gambling;
- crimes related to taxation; and
- other crimes which result in imprisonment of four years or longer.

As set forth above, tax evasion is recognised 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 8/2010 acknowledges extraterritorial jurisdiction if such foreign crime falls under one of the crimes set out in Article 2(1) (see question 1.2).

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

The Indonesian National Police and the AG have the authority to investigate money-laundering criminal offences (Article 2 of Law 8/2010). The KPK, the National Anti-Narcotics Board, the Directorate General of Taxation and the Directorate General of Customs and Excise may also have the authority (under the respective laws) to be involved in the investigation process, depending on the type of criminal offence.

Please see our response to question 1.1 for the authority to prosecute money-laundering offences at the national level.

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

Yes, Law 8/2010 provides that criminal liability for money laundering applies to both corporate and natural persons.

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

**Individuals (Article 3 of Law 8/2010)**
An individual would be subject to a maximum penalty of 20 years of imprisonment and a Rp10 billion fine.

**Legal entities (Article 7 of Law 8/2010)**
A legal entity would be subject to a maximum fine of Rp100 billion and additional penalties, which may include:
- suspension of part or all of its business activities;
- revocation of its business licence;
- dissolution and/or banning;
- forfeiture of its assets to the state; and/or
- take-over by the state.

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

Law 8/2020 is silent on the statute of limitations for money-laundering crimes. However, Article 78(1) of the Criminal Code provides a general statute of limitations, as follows:
- one year, for all misdemeanours and for crimes committed by means of the press;
- six years, for the crimes that are punished by way of fines, custody or imprisonment of a maximum of three years;
- 12 years, for all crimes that are punished by way of temporary imprisonment for more than three years; and
- 18 years, for all crimes that are punished by way of capital punishment or life imprisonment.

Accordingly, as money-laundering crimes have a maximum penalty of 20 years of imprisonment, a 12-year statute of limitation would apply.

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

The enforcement of money-laundering offences can be conducted at the national and regional (i.e. provincial) levels.

### 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 courts are the only confiscation authorities in Indonesia. If a criminal conviction has not been rendered, the confiscation of assets may only be carried out by the courts (either civil or criminal).

In general, property that is subject to confiscation consists of:
- goods or claims of the suspect or the accused of which all or part are presumed to have been obtained from an offence or as the result of an offence;
- goods that have been directly used to commit an offence or in preparation thereof;
- goods used to obstruct the investigation of an offence;
- goods specially made and intended for the commission of an offence;
- other goods which have a direct connection to the offence committed; and
- goods which have been seized due to civil suit or bankruptcy, which may also be seized for a criminal case (Article 39 of the Criminal Procedural Code).

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

Yes, there have been cases where banks or their directors, officers or employees have been convicted of money-laundering offences.

An example is the case of a Senior Relationship Manager of a prominent bank in Indonesia, who was convicted of laundering approximately Rp17 billion and sentenced to eight years of imprisonment.

### 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 offences may be settled between a victim and a suspected offender outside the judicial process, depending on the nature of the offence.

In addition, if a case of an offence meets certain requirements under Head of Police Regulation No.6 of 2019 (e.g. the case is not causing public unrest or public rejection and there has been a statement from all parties involved to not object, and waive the right to sue before the law), it can be settled through the restorative justice process instead of the judicial process.

Please note that a money-laundering offence will be processed even without any report/complaint from the victim. Accordingly, these crimes can only be resolved 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.

The Financial Services Authority ("**OJK**"), Indonesia's Central Bank ("**BI**") and the Indonesian Financial Transaction Reports and Analysis Centre ("**PPATK**") are the main government authorities responsible for issuing and imposing anti-money laundering ("**AML**") requirements to financial institutions or Financial Service Providers ("**FSP**") and other businesses.

Financial institutions or FSP are required to have policies and procedures for the implementation of the AML and Prevention of Terrorism Financing programmes, which at least encompass:
- identification and verification of the customer;
- identification and verification of a beneficial owner;
- termination of business relationship or rejection of a transaction;
- sustainable management of money-laundering and/or terrorism-financing risks in relation to the customer, country, product and service, as well as delivery channels;
- maintenance of accurate data in relation to the transaction, administration of the Customer Due Diligence ("**CDD**") process, and administration of policies and procedures;
- updating and monitoring;

- reporting to the senior officer, Board of Directors and Board of Commissioners relating to the application of policies and procedures for the implementation of AML and Prevention of Terrorism Financing programmes; and
- reporting to PPATK.

(Article 13 of OJK Regulation No.12/POJK.01/2017 as amended by OJK Regulation No.23/POJK.01/2019 ("**OJK Reg 12/2017**")).

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

There are no specific AML requirements imposed by self-regulatory organisations or professional associations. However, we note that certain organisations require their members to comply with prevailing laws and regulations in Indonesia, which include the AML provisions.

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

Self-regulatory organisations or professional associations must ensure that their members follow or implement AML requirements issued by the relevant authority (e.g. PPATK). For example, PPATK has issued PPATK Regulation No.10 of 2017 on the Implementation of Know-Your-Client Principle for Advocates, which provides compliance and enforcement regulations for advocates.

Failure to comply with AML compliance and enforcement may be deemed a violation of the ethical code of the relevant profession.

### 2.4 Are there requirements only at national level?

All requirements apply at both national and regional levels.

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

OJK, Bank Indonesia ("**BI**") and PPATK are the government institutions responsible for examining the compliance and enforcement of AML requirements.

Other government agencies may also issue AML provisions for specific sectors, including:

- the Ministry of Finance;
- the Directorate General of Domestic Trade; and
- the Commodity Futures Trading Regulatory Agency ("**BAPPEBTI**") of the Ministry of Trade.

Generally, the criteria for examination are provided in the laws and regulations and are publicly available.

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

PPATK is Indonesia's FIU. PPATK is an independent institution that was established to prevent and eradicate the practice of money laundering. It establishes its own internal policies and has the function, among others, to:

- supervise the compliance of reporting parties (e.g. financial institutions, banks, etc.); and
- analyse or examine the reports and information on financial transactions that indicate money-laundering crimes and/or their predicate crimes.

(See Article 40 of Law 8/2010.)

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

There is no statute of limitations for enforcement actions.

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

Under Article 65 of OJK Reg 12/2017, failure to comply with the regulatory/administrative requirements of submitting a report to OJK and PPATK shall result in the imposition of administrative sanctions consisting of fines in the amount of:

- Rp100,000 per day of delay per report and a maximum of Rp10,000,000 for FSP such as commercial banks, sharia commercial banks, securities companies, insurance companies, sharia insurance companies, pension funds that are managed by financial institutions, infrastructure financing companies, Indonesian export financing companies, and investment managers; or
- Rp50,000 per day of delay per report and a maximum of Rp5,000,000 for FSP such as rural credit banks, rural sharia-financing banks, financing companies, insurance brokerage companies, pawnshop companies, and venture capital companies.

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

Article 66 of OJK Reg 12/2017 provides administrative penalties, such as:

- reprimands or written warnings;
- fines, such as the obligation to pay a sum of money;
- demotion of soundness assessment level;
- limitation of certain business activities;
- suspension of certain business activities;
- for banks, termination of the management and further designating and appointing a temporary substitute until a general meeting of shareholders or a meeting of the members of the cooperative appoints a permanent substitute approved by the OJK; and/or
- inclusion of the members of the Board of Directors and members of the Board of Commissioners, employees of PJK, and shareholders into the financial services sector blacklist.

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

Penalties for violations of anti-money laundering obligations include both administrative sanctions (under OJK Reg 12/2017) and criminal penalties (under Law 8/2010).

Please see our responses to questions 1.6, 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 process for the assessment and imposition of administrative sanctions for any violation of OJK Reg 12/2017 will be carried out by OJK.

For administrative sanctions such as fines, the FSP is required to pay such fine to OJK's bank account or by other payment method required by OJK no later than 30 days after OJK issues a Sanction Letter Administrative Fine (OJK Regulation No.4/POJK.04/2014 as lastly amended by OJK Regulation No.26/POJK.02/2018).

Generally, upon the imposition of such administrative sanction, the relevant FSP would usually meet with OJK or PPATK officials to discuss any disagreements or objections to such imposition. However, in practice it is unlikely that an entity will challenge a penalty/sanction assessment.

## 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.**

Government Regulation No.43 of 2015 and OJK Reg 12/2017 specifically provide that the term "FSP" (or "financial institutions") covers:

- FSP within the banking sector: commercial banks, including sharia commercial banks, rural credit banks, and rural sharia-financing banks as addressed under the laws and regulations on the banking sector;
- FSP within the capital market sector: securities companies, including underwriters, brokers, and/or investment managers, as well as commercial banks that operate custodian functions; and
- FSP within the non-bank financial industry sector: insurance companies; sharia insurance companies; insurance brokerage companies; pension funds; financing companies; venture capital companies; infrastructure-financing companies; Indonesian export financing companies; pawnshops; micro financial companies; and the organisers of money-lending services on the basis of information technology as referred to under the laws and regulations within the non-bank financial industry.

In addition, Government Regulation No.43 of 2015 also states that professionals, such as lawyers, notaries, land deed officials and accountants are subject to AML requirements.

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

The cryptocurrency industry is under the supervision of BAPPEBTI.

BAPPEBTI issued BAPPEBTI Regulation No.9 of 2017 in relation to AML compliance for futures brokers (*pialang berjangka*). Under such regulation, a futures broker is obliged to implement AML measures, prevent terrorism-financing programmes and comply with reporting obligations to PPATK.

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

Yes, FSP must maintain and conduct anti-money laundering and terrorism financing eradication programmes. Please see our response to question 2.1.

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

Under OJK Reg 12/2017, an FSP must submit reports on suspicious financial transactions, reports on financial transactions in cash and other reports to PPATK as set out under Law 8/2010.

One of the criteria for a transaction that must be reported to PPATK is if there is a transaction in cash in the amount of at least Rp500,000,000 or its equivalent in another currency which is made in a single transaction or multiple transactions on business days (Article 23(1) of Law 8/2010), except for:

(a) any transaction made between the FSP and the government and/or the central bank;
(b) transactions for payment of salaries and pensions; and
(c) other transactions stipulated by the Chairman of PPATK or upon the request of the FSP that has been agreed by the Chairman of PPATK.

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

In addition to the requirements set out in our response to question 3.4, an FSP must also submit a report to PPATK if there is a:

(a) suspicious financial transaction (please refer to our response to question 3.9); and/or
(b) cross-border transfer of funds (both from and to foreign countries).

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

Yes, please see our response to question 3.5.

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

An FSP must implement a CDD procedure when:

- engaging in a business relationship with a prospective customer;
- there is a financial transaction using IDR currency and/or foreign currencies with a minimum or equivalent value of Rp100 million;

- there is a Fund Transfer transaction as referred to under OJK Reg 12/2017;
- there is an indication of suspicious financial transactions relating to money laundering and/or the financing of terrorism; or
- FSP doubts the validity of information that is provided by a prospective customer, customer, proxy, and/or beneficial owner.

(Article 15 of OJK Reg 12/2017.)

In addition to the above, FSP must perform CDD on beneficiaries of life insurance and other investment products related to insurance policies, soon after the beneficiary is identified or established (Article 37(1)).

An FSP must categorise prospective customers and customers based on their risk levels on the occurrence of money laundering and/or terrorism financing. The classification of risk levels shall be performed based on an analysis which at least encompasses: (i) the identity of the customer; (ii) the business domicile, for corporate customers; (iii) the profile of the customer; (iv) the frequency of transactions; (v) the business activities of the customer; (vi) the ownership structure, for corporate customers; (vii) the product, service, and delivery channels that are used by the customer; and (viii) other information which may be used to measure the risk levels of the customer.

**Simple CDD**

FSP may implement simple CDD procedures on a prospective customer or transaction that has a low level of risk in relation to the occurrence of money laundering and/or financing of terrorism and satisfies certain criteria under Article 40.

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

Yes, an FSP is prohibited from carrying out business with a prospective customer and/or carrying out transactions with a walk-in customer if such prospective customer or walk-in customer is a shell bank or commercial or sharia commercial bank that allows its accounts to be used by a shell bank (see Article 42 of OJK Reg 12/2017).

In addition, a delivering bank that provides cross-border correspondent banking services must also refuse to engage and/or forward the cross-border correspondent banking relationship with a shell bank. Further, such delivering bank must also ensure that the receiving bank and/or the intermediary bank does not allow its account to be used by a shell bank when conducting a business relationship in relation to cross-border correspondent banking.

### 3.9 What is the criteria for reporting suspicious activity?

OJK Reg 12/2017 provides the criteria for reporting suspicious financial transactions as defined under Law 8/2010, as follows:

(a) transactions that deviate from the profile, characteristics or habit of the usual transaction pattern of the relevant customer (or service user);
(b) transactions that are reasonably suspected of being carried out for the purpose of avoiding the reporting requirement for the relevant transaction (which the reporting party is obligated to do in accordance with the provision under OJK Reg 12/2017);
(c) a successful or a failed transaction using assets that are suspected of having originated from a criminal action; or
(d) a transaction that is specifically requested by PPATK to be reported by the reporting party because the transaction is believed to involve assets originating from a criminal action.

The submission of the report of suspicious financial transactions above shall be performed as soon as possible, no later than 3 days after the FSP knows the presence of elements of suspicious financial transaction. Law 8/2010 is silent on the exception for this reporting obligation.

Any violation to this reporting obligation will be subject to administrative sanctions in the form of a: (i) warning; (ii) written warning; (iii) announcement to the public regarding the action and/or penalty; and/or (iv) fine.

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

In general, the Ministry of Law and Human Rights ("**MoLHR**") maintains general information or profile of a legal entity, namely its capital structure, shareholders and organs ("**Company Profile**"). Such Company Profile, however, does not contain any information about beneficial ownership of such legal entity.

To obtain this Company Profile, one can access the MoLHR website (http://ahu.go.id) and pay a fee (which constitutes non-tax state revenue) in the amount of: (i) Rp500,000 for a complete Company Profile; or (ii) Rp50,000 for the most recent Company Profile.

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

Article 8 of Law No.3 of 2011 provides that funds transfer orders (including to other financial institutions) should at least contain:

(a) the identity of the originator;
(b) the identity of the beneficiary;
(c) the amount and type of currency;
(d) the date of the funds transfer order; and
(e) other required information set out under the laws and regulations related to funds transfers (i.e. OJK Reg 12/2017).

Under OJK Reg 12/2017, the above requirement does not apply to: (i) funds transfers using debit cards, ATM cards or credit cards; or (ii) funds transfers between FSPs and for the interest of such FSP.

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

Article 48 of Law No.40 of 2007 provides that a company's shares must be issued under the names of the owners of such shares.

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

Legal entities in Indonesia are now required to declare the identity of beneficial owners and provide information on their

beneficial ownership to prevent and eradicate money-laundering offences and criminal acts of terrorism financing as required under Presidential Regulation No.13 of 2018.

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

Please see our response to question 2.1.

In addition, please note that any person carrying cash (both in Rupiah and/or foreign currencies) and/or other payment instruments (e.g. checks, travel checks, promissory notes) in the amount of at least Rp100,000,000 or its equivalent in another currency into or outside the Indonesian customs area must declare such cash and/or other payment instruments or notify the Directorate General of Customs and Excise of the same (Article 34 of Law 8/2010).

## 4 General

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

In 2019, the government of Indonesia, through cooperation at the regional level with the Financial Intelligence Units of all ASEAN countries, Australia and New Zealand, commenced assessment of the threat of transnational money laundering of funds sourced from criminal acts of corruption. The mapping of threats to be identified consists of profiles, industry groups, economic sectors, types of corruption and country interactions. This threat level assessment is still ongoing.

**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 Mutual Evaluation in 2018, Indonesia was deemed Compliant for six and Largely Compliant for 29 of the FATF 40 Recommendations. It was deemed Highly Effective for zero and Substantially Effective for five of the Effectiveness & Technical Compliance ratings.

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

Indonesia, as a member of the Asia Pacific Group on Money Laundering ("**APG**") and an observer country to the FATF, is under evaluation by the FATF.

The last Mutual Evaluation follow-up Report in relation to the implementation of anti-money laundering and counter-terrorist financing standards in Indonesia was undertaken in 2018 (https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-Mutual-Evaluation-Report-Indonesia.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?**

At this stage, Indonesia does not have any integrated system on AML laws and regulations. In order to locate such laws and regulations, one can access the relevant government institution's website, such as the Secretariat of Cabinet of the Republic of Indonesia's website (https://jdih.setkab.go.id/), the OJK website (https://ojk.go.id/id/Regulasi/Default.aspx), BI's website (https://www.bi.go.id/id/peraturan/pencarian-peraturan/Default.aspx) and PPATK's website (http://jdih.ppatk.go.id/).

Please note that AML laws and regulations are generally not available in the English language.

**Ardian Deny Sidharta** (**Deny**) is a partner of S&T whose main areas of practice include energy, resources and infrastructure, environment and forestry, public-private partnerships ("**PPPs**"), general corporate and investment, and anti-corruption.

**Soemadipradja & Taher**
Wisma GKBI, Level 9
Jl. Jend. Sudirman No.28
Jakarta, 10210
Indonesia

Tel: +62 21 574 0088
Email: deny_sidharta@soemath.com
URL: www.soemath.com

**Erie H. Tobing** (**Erie**) is a partner at S&T whose main areas of practice include bankruptcy and suspension of payment, maritime, banking & finance, construction, commercial transactions, general litigation, and alternative dispute resolution.

**Soemadipradja & Taher**
Wisma GKBI, Level 9
Jl. Jend. Sudirman No.28
Jakarta, 10210
Indonesia

Tel: +62 21 574 0088
Email: erie_tobing@soemath.com
URL: www.soemath.com

**Oene J. Marseille** is a partner of the leading Singaporean law firm Allen & Gledhill ("**A&G**") and is currently assigned to S&T as part of the strategic alliance between S&T and A&G. His main practice areas are M&A and corporate and commercial transactions.

**Soemadipradja & Taher**
Wisma GKBI, Level 9
Jl. Jend. Sudirman No.28
Jakarta, 10210
Indonesia

Tel: +62 21 574 0088
Email: oene_marseille@soemath.com
URL: www.soemath.com

**Aris Budi Prasetiyo** is an international counsel at A&G who is currently assigned to S&T as part of the strategic alliance between S&T and A&G. His areas of practice include M&A, general corporate and banking.

**Soemadipradja & Taher**
Wisma GKBI, Level 9
Jl. Jend. Sudirman No.28
Jakarta, 10210
Indonesia

Tel: +62 21 574 0088
Email: aris_prasetiyo@soemath.com
URL: www.soemath.com

Established in 1991, Soemadipradja & Taher ("**S&T**") is consistently ranked top tier among Indonesian law firms. Our firm consists of 11 partners, three foreign counsels, one special counsel and 35 associates.
Through the collective expertise of our partners, counsels and lawyers, a wealth of experience representing corporate clients, and an ability to look beyond traditional approaches and think creatively, we assist national, foreign and multinational clients to achieve their business objectives in Indonesia.
As specialists in providing corporate legal services, we understand our clients' businesses, industries and corporate goals, ensuring that we provide the most appropriate legal solutions adjusted to our clients' needs, while applying the highest ethical and professional standards.

S&T has formed a strategic alliance with Allen & Gledhill of Singapore, and maintains relationships with a number of leading regional and international law firms, including Corrs Chambers Westgarth and Nagashima Ohno Tsunematsu.

**www.soemath.com**

S&T Advocates
Soemadipradja & Taher

# Isle of Man



Kathryn Sharman


Michael Nudd


Sinead O'Connor

DQ Advocates Limited


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the 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 committed on the Island. A section 139 offence is the offence of concealing, disguising, converting, transferring or removing criminal property from the Island. A section 140 offence is the offence of becoming concerned in an arrangement which the person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. A section 141 offence is the offence of acquiring, using or having possession of criminal property. Property is criminal property if: (i) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or in part and whether directly or indirectly); and (ii) the alleged offender knows or suspects that it constitutes or represents such a benefit. Criminal conduct is conduct which: (a) constitutes an offence in the Island; or (b) would constitute an offence in the Island if it occurred there.

POCA does not specify which predicate offences are included but as the predecessor legislation extended to all crimes, POCA would apply to any crime which generated money to be laundered. This is inclusive of tax evasion.

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

There are provisions within POCA for enforcement of a confiscation order where the property in question is outside of the Island or there may be evidence of criminal conduct outside the Island. There are also provisions for co-operation with external authorities who make requests for assistance. As set out in question 1.2, if the criminal conduct occurred outside of the Island, it is punishable if the criminal conduct would constitute an offence in the Island if it occurred there.

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

It is the responsibility of the Economic Crime Unit to investigate money laundering offences, which then in turn passes the information to the Attorney Generals Chambers for prosecution (as applicable).

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

Section 221 of POCA states that where an offence under the Act is committed by a body corporate and it is proved that the offence: (a) was committed with the consent and connivance of an officer of the body; or (b) was attributable to neglect on the part of an officer of the body, the officer, as well as the body, shall be guilty of the offence.

There is also corporate criminal liability under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 (as amended 2019) (the "Code"). The Code is secondary legislation made under POCA which requires relevant businesses to have anti-money laundering and countering the financing of terrorism procedures and controls in place.

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

A person guilty of an offence as set out in question 1.2 above is liable on summary conviction to custody for a term not exceeding 12 months, or to a fine not exceeding £5,000, or both; or on conviction on information, to custody for a term not exceeding 14 years, or to a fine or both.

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

There is no prescribed statute of limitations in respect of criminal conduct which can give rise to criminal property.

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

Enforcement is only at national level. There are no states or provinces in the Isle of Man.

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

POCA provides for recovery orders, property freezing orders, interim receiving orders, recovery of cash, confiscation orders and restraint orders.

Proceedings for a recovery order may be taken by the Attorney General in the High Court against any person who the Attorney General thinks holds recoverable property. There are extensive provisions in POCA as to what is and is not recoverable property but it is, in essence, property obtained through unlawful conduct.

Where the Attorney General may take proceedings for a recovery order in the High Court, the Attorney General may apply to the court for a property freezing order. He may also apply for an interim receiving order.

There are provisions for the seizure and detention of cash if a customs officer or police constable suspects that the cash is recoverable property or is intended for use by any person in unlawful conduct.

The Court of General Gaol Delivery can make a confiscation order if it (a) decides that the defendant has a criminal lifestyle and has benefitted from his or her general criminal conduct, or (b) it decides that the defendant does not have a criminal lifestyle and has benefitted 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.

In addition to the criminal offence of Money Laundering, the Anti-Money Laundering and Countering the Financing of Terrorism (Civil Penalties) Regulations 2019 allow for the imposition of a fine for money laundering or terrorist financing-related failings. To date, an insurance company and a corporate service provider have been issued civil fines under the scheme.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

Aside from the primary legislation (POCA, the Anti-Terrorism and Crime Act 2003 and the Terrorism and Other Crime (Financial Restrictions) Act 2014), the Code, as referred to in question 1.5, also imposes AML requirements on financial institutions and other businesses. In addition, the Isle of Man Financial Services Authority (the "FSA"), which is the principal supervisor of financial institutions and designated non-financial businesses and professions ("DNFBPs"), has issued a comprehensive AML/CFT Handbook (the "Handbook") which sets out how the provisions of the Code should be met.

The Gambling Supervision Commission (the "GSC") is the principal supervisor of the e-gaming and terrestrial gaming sector. Whilst the primary legislation applies equally to the gambling sector, there is a gaming-specific version of the Code and also a separate AML/CFT Handbook issued by the GSC.

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

It is likely that the professional associations in the accountancy sector have anti-money laundering requirements which are

imposed on member firms in the Isle of Man. As these requirements are UK-based and do not take account of Isle of Man AML/CFT legislation and regulation, compliance with the Isle of Man standards will normally ensure compliance with any UK-based standards. Island members of such professional associations would normally look to the FSA's Handbook for the standards of conduct expected.

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

The FSA is the principal supervisor of all financial institutions and DNFBPs. Although supervision through on-site visits of some of the DNFBPs has been delegated to the self-regulatory organisations or professional associations with which the FSA has a Memorandum of Understanding, the FSA remains responsible for enforcement.

**2.4 Are there requirements only at national level?**

Due to the size of the Isle of Man, there are only requirements at national level.

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

The FSA is responsible for examination of compliance and enforcement of anti-money laundering requirements for financial institutions and DNFBPs. The GSC is responsible for examination of compliance and enforcement of anti-money laundering requirements for gaming operators. The FSA's supervisory approach is normally publicly available. That of the GSC does not appear to be publicly available.

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

There is a Financial Intelligence Unit (the "FIU") which is under the direction of a Board comprised of the Attorney General, the Chief Constable and the Collector of Customs & Excise. Financial institutions, DNFBPs and gaming operators are all required to report to the FIU via the online portal THEMIS.

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

There is no prescribed limitation upon which a competent authority must bring enforcement actions under legislation.

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

A breach of the Code and its gaming equivalent carries a penalty of: (a) on summary conviction to custody for a term not exceeding 12 months or to a fine not exceeding £5,000 or both; or (b) on conviction on information, to custody not exceeding two years or to a fine or both. The FSA has powers under the Financial Services (Civil Penalties) Regulations 2015 and the Anti-Money Laundering and Countering the Financing of Terrorism (Civil Penalties) Regulations 2019 to levy a civil penalty. Where there is a Level One issue (risk of loss), the FSA can fine the licence holder up to 5% of relevant income. Where there is a Level Two issue (actual loss), the FSA can fine the licence holder up to 8% of relevant income. The FSA has used its new civil powers in respect of two licence holders who were convicted of a breach of the Code. The penalties levied by the courts for breach of the Code were in the region of £51,000 and £57,000. 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 2019 provides the GSC with similar powers to the FSA, including the ability to levy civil penalties. The 2019 Civil Regulations do not extend to the GSC.

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

The FSA and the GSC have a range of sanctions available to them including restriction of activities, licence conditions, directions, public statements, injunctions, warning notices, appointment of skilled persons, prohibitions and revocation of the licence.

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

A breach of the Code would be criminal, as would any offence under the primary legislation.

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

There is an appeal process set out in the Financial Services Act 2008 in relation to decisions made by the FSA. There is a Financial Services Tribunal which would hear any appeal. Some measures taken by the FSA, for example, a warning notice, might not be made public but an appeal to the Tribunal would usually be in the public domain. Similarly, there is a Gambling Appeals Tribunal which would hear any appeal under the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2019.

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

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

Schedule Four to POCA sets out which types of business qualify as a 'business in the regulated sector' for the purposes of POCA

and the Code. There is a wide range of businesses captured which includes the traditional financial services sector (banking, insurance, funds), as well as the gaming sector (online and terrestrial), estate agents, lawyers (when they undertake certain types of activities), accountants, corporate and trust service providers, pension providers, money transmission agents, tax advisers, charities, payroll agents and those businesses involved with virtual currency.

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

As per the answer to question 3.1, businesses involved with virtual currency are deemed to be a business in the regulated sector and have to comply with the Code. The wording of Section Four of POCA is widely drawn and encompasses the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies including crypto currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or a commodity. Any business which falls into this definition must register with the FSA as a DNFBP and is subject to the FSA's supervision for compliance with the Code and the FSA's AML/CFT Handbook.

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

Any business which qualifies as a 'business in the regulated sector' (see question 3.1 above) is required to comply with the Code. Paragraph 30 of the Code requires such a business to maintain appropriate procedures for monitoring and testing compliance with the AML/CFT requirements, having regard to ensuring that: (a) the business has robust and documented arrangements for managing the risks identified by the business risk assessment; (b) the operational performance of those arrangements is suitably monitored; and (c) prompt action is taken to remedy any deficiencies in arrangements.

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

In accordance with the Customs & Excise Management Act 1986, Customs & Excise issued Notice 9011 (the "Notice") in November 2008. The Notice states that if cash in excess of €10,000 is sent to or taken from, or is brought into or received in the Island, then the person carrying, sending or receiving it must make a declaration to Customs & Excise. This applies to cash going to or coming from anywhere outside the Island and regardless of whether the cash is being carried by someone or is sent in the mail, by courier service or is contained in freight, a vehicle or a vessel. Cash includes any banknotes or coins in any currency (including counterfeit), postal orders and cheques of any kind (including travellers' cheques) but excluding cheques drawn on a British or Irish bank. It also includes stored value cards, and other documents, devices, coins or tokens with a monetary value.

Paragraph 13 of the Code requires a business in the regulated sector to perform ongoing and effective monitoring of any business relationship which includes appropriate scrutiny of transactions, paying particular attention to suspicious and unusual activity. Unusual activity is defined in the Code to include large transactions. There is no definition or threshold for 'large', so each business would have to consider that in the context of their customer relationship.

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

There is a requirement to report any suspicious transaction to the FIU.

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

Aside from the requirements of Notice 9011 set out in question 3.4, Isle of Man financial institutions also have to comply with the US Foreign Account Tax Compliance Act and the Common Reporting Standard. These require automatic exchange of information on accounts and balances held by residents of various other jurisdictions. Reporting by Isle of Man financial institutions is to the Isle of Man Income Tax Division which then exchanges the information with other tax authorities around the world.

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

The customer due diligence requirements are set out in the Code. These broadly require: (a) the identification of the customer; (b) the verification of the identity of the customer using reliable, independent source documents; (c) the verification of the legal status of the customer using relevant information obtained from a reliable independent source; (d) the obtaining of information on the nature and intended purposes of the business relationship; and (e) the taking of reasonable measures to establish the source of funds. The FSA's Handbook provides further guidance on each of these areas.

Enhanced customer due diligence ("EDD") must be obtained (a) where a customer poses a higher risk of ML/TF as assessed by the customer risk assessment, or (b) in the event of any unusual activity. EDD is only required for a politically exposed person if there is a higher risk of ML/TF.

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

Paragraph 38 of the Code states that a business subject to the Code must not enter into or continue a business relationship or occasional transaction with a shell bank. Such a business must also take adequate measures to ensure that it does not enter into or continue a business relationship or occasional transaction with a respondent institution that permits its accounts to be used by a shell bank.

**3.9 What is the criteria for reporting suspicious activity?**

Section 142 of POCA creates the failure to disclose an offence on the basis of four conditions being present. These are, in summary: (1) there is knowledge or suspicion or reasonable grounds for knowing or suspecting that another is engaged in money laundering; (2) that knowledge or suspicion or reasonable grounds came from business in the regulated sector; (3) the identity of the person mentioned in (1) or the whereabouts of the laundered property is known or there is information that may assist in that regard; and (4) a disclosure is not made to the FIU.

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

Under the Beneficial Ownership Act 2017, there is a central register of beneficial owners of Isle of Man companies. This is, however, a private register and is only available to certain authorities via formal requests. It is not accessible by Isle of Man financial institutions other than to enter their own information.

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

The Island has implemented the EU Directive in relation to wire transfers through an Order and Regulations. In accordance with the Directive, the ordering financial institution has to ensure that all wire transfers carry specified information about the originator (Payer), who gives the instruction for the payment to be made, and the Payee, who receives the payment. The core requirement is that the Payer information consists of name, address, account number, official personal document number, customer identification number or date and place of birth, and that the Payee information consists of name and account number. There are also requirements imposed on any intermediary payment service providers.

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

The Companies (Prohibition of Bearer Shares) Act 2011 provides that bearer shares are not permitted as a form of ownership of legal entities and under the AML/CFT requirements, the existence of bearer shares in a non-Isle of Man incorporated entity should be considered as a risk factor.

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

As per question 3.1, there is a wide range of businesses which have to comply with the Code. These include DNFBPs and so there are no other categories of business which have additional AML requirements.

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

There is nothing additional for what is required under the primary legislation, the Code and associated guidance. It is important, however, to note that the Island has a range of Sanctions Notices in place in accordance with United Nations measures and the EU financial and economic sanctions. Isle of Man businesses are prohibited from doing business with any entity or individual named on a Sanctions Notice and must also be familiar with the conditions of doing business with sanctioned countries.

## 4 General

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

There are a number of other proposed changes including the proposed Regulations referred to in question 2.8, changes to certain parts of the primary legislation and changes to the Designated Businesses (Registration and Oversight) Act 2015. There is also a separate Code being consulted on for not-for-profit organisations.

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

MONEYVAL published a 2nd Enhanced Follow up report on the Isle of Man in July 2019. It detailed that there has been progress made in addressing the technical compliance deficiencies identified in the 5th Mutual Evaluation Report. Some Recommendations ratings have been regraded to a high standard of compliance, which is incredibly positive and shows that the Isle of Man is becoming more compliant. However, not all deficiencies have been addressed and the Isle of Man is encouraged to continue its efforts to address such deficiencies. Currently, the Isle of Man remains in the enhanced follow-up process and is due to report back to MONEYVAL in 2020.

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

Please see question 4.2.

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

A good summary is set out in Part 7 of the FSA's Handbook. This is available on the FSA's website and is in English. The Handbook contains a copy of the Code. Primary legislation is available from the Attorney General's Chambers website and it is also in English.

**Kathryn Sharman** is a Trainee Advisor in the Regulatory and Compliance Team. She regularly advises on AML/CFT compliance, in addition to other financial service-related compliance matters.
Kathryn has an LL.B. degree and is currently working towards the ICA Anti-Money Laundering Diploma.

**DQ Advocates Limited**
The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 632 967
Email: kathryn.sharman@dq.im
URL: www.dq.im

**Michael Nudd** is a consultant supporting the Regulatory Compliance Services team.
Mike was originally in banking, working for 24 years in a UK clearing bank. Since coming to the Isle of Man in 1998, Mike has worked in the finance sector with the Regulator, in Banking, Funds and also the Trust and Corporate Services industry.
Mike is a Fellow of the International Compliance Association and has extensive industry knowledge and experience.

**DQ Advocates Limited**
The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626 999
Email: michael.nudd@dq.im
URL: www.dq.im

**Sinead O'Connor** 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.

**DQ Advocates Limited**
The Chambers, 5 Mount Pleasant
Douglas, IM1 2PU
Isle of Man

Tel: +44 1624 626 999
Email: sinead@dq.im
URL: www.dq.im

# Japan



Ryu Nakasaki


Kei Nakamura

Nakasaki Law Firm


## 1 The Crime of Money Laundering and Criminal Enforcement

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

Money laundering is criminalised by Article 10 of the Act on Punishment of Organized Crimes and by other related acts. The authority to prosecute money laundering belongs to the prosecutors.

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

The elements for the offence of money laundering are:

(1) disguising facts pertaining to the sources, acquisition, or disposition of "Criminal Proceeds, Etc." (see question 1.9);
(2) hiding of Criminal Proceeds, Etc.; or
(3) (i) acquiring shares or ownership of an entity to control such entity using Criminal Proceeds, Etc., and (ii) executing such shares or ownership to appoint or remove any director or other management member, or to change representative director or similar officer.

Accomplices and accessories to such crimes are also punishable.

The predicate offences of criminal proceeds include a variety of crimes, including but not limited to all crimes which may result in four years' (or more) imprisonment.

Yes, tax evasion crimes are predicate offences.

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

Yes, there is a provision of extraterritorial jurisdiction for the crime of money laundering (e.g. Article 12 of the Act on Punishment of Organized Crimes and Control of Crime Proceeds). Yes, money laundering of the proceeds of foreign crime is subject to punishment in Japan.

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

(i) The National Police Agency ("NPA"), and (ii) the government agency supervising the applicable industry area (e.g. Financial Services Agency for the bank industry) are both responsible for making investigations and for imposing administrative penalties. Furthermore, 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 is five years.

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

Yes, enforcement is only at national level.

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

Yes. The court administers forfeiture procedures.

All property that falls under any of the following ("Criminal Proceeds, Etc.") may be confiscated:

(i) instrumentalities of predicate offence or money laundering or proceeds of crime, including remuneration for crime ("Criminal Proceeds");
(ii) property that is acquired in exchange for Criminal Proceeds; or
(iii) 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, but such cases are rare.

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

Criminal actions regarding money laundering are resolved through judicial processes.

A reform of the Code of Criminal Procedure in 2018 has enabled a plea-bargain. Records of judgment can be viewed at the court.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

The "Act on Prevention of Transfer of Criminal Proceeds" ("AML Act") is the basic law that provides for AML.

Financial institutions and designated non-financial business 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; provided, however, that lawyers do not need to submit SARs.

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

Yes. Self-regulatory organisations including those of financial institutions and DNFBPs generally set forth additional requirements. For example, the Japan Federation of Bar Associations implements a rule on AML measures to be taken by lawyers.

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

Yes, they are.

**2.4 Are there requirements only at national level?**

Yes. There are no AML requirements imposed at the local government level. Please note, however, that some local governments, including prefectures, demand business entities not to transact with criminal organisations and the like (or in other words, "antisocial forces").

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

Please see question 1.4 regarding the government agencies that are responsible for the examination for compliance and enforcement of AML requirements. There are some publicly available examination criteria. For example, the Financial Services Agency has issued a guideline pertaining to AML/CTF measures to be taken by financial institutions.

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

Yes, the Financial Intelligence Centre of the NPA ("FIC") is the FIU in Japan. The FIC publishes an annual report of the result of its analysis of money-laundering activities in Japan.

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

There is no statute of limitation for administrative enforcement actions. For criminal actions, the statute of limitations is three years.

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

The maximum penalty under the AML Act for individuals is imprisonment up to two years and a fine of up to three million yen. The maximum penalty for a legal entity 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 a licence, (ii) order for suspension of business, and (iii) order for rectification.

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

Penalties for violations can be both administrative/civil as well as subject to criminal sanctions.

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

Process for assessment: administrative sanctions are imposed by

supervising authorities with prior notice and hearing, but fines cannot be imposed.

Process of collection of sanctions: no fine as an administrative sanction.

Process of appeal of administrative decisions: one may file a request to review the administrative decision to the supervising authority itself under Article 6 of the Administrative Complaint Review Act. If the supervising authority does not change the decision, a lawsuit may then be filed to cancel such administrative decision under Article 8 of the same act.

a) Not all administrative decisions are made public.
b) This is very rare but has happened.

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

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

Financial institutions including banks, securities companies, insurance companies, lending businesses, fund transfer businesses, credit card issuing companies, and finance lease companies, among others, are subject to AML regulations, as well as DNFBPs including lawyers, accountants, real estate brokers, jewellery dealers, company service providers and such.

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

Cryptocurrency exchanges are subject to AML requirements as "crypto asset exchanges". Transactions as "crypto asset exchanges" are subject to AML requirements, just as are other obliged entities. Please note that cryptocurrency exchanges registered in Japan basically do not interpret themselves as money transmitters in relation to Japanese law, and therefore they basically judge that Japanese AML regulations on wire transfer and money transmitters are not applicable to themselves.

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

Yes, compliance programmes are required (e.g. Article 11 of the AML Act, Article 348(3)(iv), etc. of the Companies Act, Article 12-2 of the Banking Act).

The compliance programme is expected to include the following items, among others:

(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 on such analysis, and updating such reports;
(6) monitoring of CDD records and transaction information to detect suspicious activities;
(7) taking measures to ensure that competent and appropriate staff members are hired or allocated;
(8) conducting audits;
(9) implementing measures to keep the records of customers up to date; and
(10) implementing AML measures equivalent to those required under Japanese law at its overseas subsidiaries and branches.

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

There is a seven-year record-keeping requirement for "customer verification records" and for "transaction records". There are some exemptions to this requirement for transaction records, including an exemption for transactions pertaining to the transfer of property with a value equal to or less than 10,000 yen.

For reporting of large currency transactions, casinos will be subject to a large currency report, but other businesses are basically not subject to such report.

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

For reporting of cross-border payment transactions, please see question 3.6.

In addition to such reporting, financial institutions need to submit various reports pursuant to the Foreign Exchange and Foreign Trade Act. For example:

- Article 55-3 and 55-4 provide for reports for capital transactions and the like; and
- Article 55-7 provides for reports on foreign exchange operations.

However, most of these reports may be submitted by a financial institution, in aggregate form, on a monthly, quarterly or annual basis depending on the type of report.

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

For cross-border funds transfer in the amount exceeding 1 million yen (or equivalent in other currencies), the relevant financial institution must submit a "Statement of Overseas Wire Transfer" (Article 4 of the Act on Submission of Statement of Overseas Wire Transfers for Purpose of Securing Proper Domestic Taxation).

For cross-border payments or set-offs in the amount exceeding 30 million yen, the resident in Japan, that is, either the payor or the payee, needs to submit a payment report to the government (Article 55 of the Foreign Exchange and Foreign Trade Act). Please note that if the payment is made through an office or branch in Japan of a bank or fund transfer business, such report will be submitted through such financial institution.

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

**1. Normal CDD**

In conducting transactions designated by the AML Act as subject to customer verification (or "Designated Transactions"), obliged entities need to verify the following matters in the following methods.

| Matters to be Verified | Verification Method |
|---|---|
| Identification of Customers (*) | Need to be verified using ID documents.<br>The verification methods include, among others: (1) having the customer present photo-ID documentation; (2) having the customer send two kinds of ID documentation and send untransferable registered mail to the address of the customer on the ID document verified; and (3) eKYC, which was made available after the 2018 amendment of the AML Act Cabinet Ordinance.<br>The rules for the verification methods are very complex. |
| Authority as Agent | Verification using records of commercial registry and such. |
| Purpose of the Transaction | Having the customer declare. |
| Occupation (for Individual)/ Business (for Legal Entity) | Having the customer declare. |
| Identification of its Representative, etc. (for Legal Entity and such) | Need to be verified using ID documentation. |
| Identification of Beneficial Owner (for Legal Entity) | Having the customer declare. |

* "Identification of Customers" means the name, address, and birth date for individual customers, and means the name and address of its main office for legal entity customers.

**2. Enhanced CDD**

In conducting transactions that fall under any of the following transactions, Enhanced CDD is required:

(1) transactions where ID fraud is suspected, which has arisen from a Designated Transaction;
(2) transactions where ID theft is suspected, which has arisen from a Designated Transaction;
(3) Designated Transaction with Foreign PEPs, Etc.; or
(4) Designated Transaction with a resident in a high-risk country (e.g. Iran or North Korea) or a Designated Transaction where funds are transferred to a high-risk country.

| Matters to be Verified | Verification Method |
|---|---|
| Identification of Customers | Same as normal CDD. |
| Authority as Agent | Same as normal CDD. |
| Purpose of the Transaction | Same as normal CDD. |
| Occupation (for Individual)/ Business (for Legal Entity) | Same as normal CDD. |
| Identification of its Representative, etc. (for Legal Entity) | Same as normal CDD. |
| Identification of Beneficial Owner (for Legal Entity) | Verification using annual securities report, top 10 shareholders' list, etc. |
| Asset and Income (in Transferring Assets that Exceed 2 Million Yen) | Verification by financial statements, etc. |

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

Establishment of a shell bank is not permitted in Japan. Also, banks and fund transfer businesses licensed or registered in Japan are required to make investigations as to whether the financial institution that it will enter into a correspondent agreement with is a shell bank or not (Article 9 of the AML Act).

**3.9 What is the criteria for reporting suspicious activity?**

There are basically two types of transactions that are subject to the submission of SARs. The first is transactions where the funds that the relevant financial institution or the DNFBP receives from the customer is suspected to be Criminal Proceeds, Etc. The other is transactions where the customer is suspected to be engaging in money laundering. Also, government agencies supervising each type of Obliged Entity usually issue examples of transactions that would require the filing of SARs.

Lawyers, accountants and similar professions are exempted from submitting SARs. They may submit SARs when they deem it necessary, but they are not obliged to do so under Japanese law.

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

Japanese legal entities are registered in the commercial registry administered by the government. However, the names of shareholders and the beneficial owner are not to be registered in the commercial registry.

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

Yes, for both questions (Article 10 of the AML Act). Please

note that this article will apply to bank wire transfers but will not likely apply to card transactions (e.g. through Visa and MasterCard), as described in the Interpretive Notes to FATF Recommendation 16.

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

Yes. The provision in the Companies Act referring to bearer shares has been abolished, although stating the name of the holder on a share certificate is not obligatory (Article 216 of the Companies Act), thus bearer shares do exist and are not prohibited.

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

Basically, no. However, there are some differences, for example in relation to casinos and the like.

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

(1) In relation to the AML Act, the general rules for AML basically do not apply to lawyers; the rules of the Japan Federation of Bar Associations are applied instead. This creates some difference, but it is not that significant.

(2) In relation to the Foreign Exchange and Foreign Trade Act, banks and funds transfer businesses are required to conduct CDDs when providing cross-border wire transfer or other funds transfer services to its customers.
Also, banks, securities companies, currency exchange businesses, and certain other types of financial institutions are obliged to conduct CDDs when providing services regarding certain cross-border capital transactions, including but not limited to loans, acceptance of deposits, and currency exchange. The CDD measures required under the Foreign Exchange and Foreign Trade Act are basically equivalent to the CDD measures required under the AML Act.

(3) Under tax-related laws, banks and securities companies are basically required to ask the 'My Number' (which is a social security and tax number given to each individual resident by the Japanese government) when opening an account. Financial institutions will verify the My Number using the My Number Card held by such customer or by a copy thereof. Please note that the My Numbers need to be held in strict confidentiality.

## 4 General

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

No proposal is being publicised at present. However, after the FATF mutual evaluation report on Japan is publicised (see question 4.3), we expect that some amendment to the AML Act will be enacted to implement changes recommended by FATF in such report.

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

Yes, there are.

(1) Ongoing CDD measures are not required under the AML Act. For financial institutions, there is a provision in the AML guideline demanding such measures, but there is no such guideline for most non-financial institutions.

(2) Transactions with "Domestic" Politically Exposed Persons are not high-risk transactions. For other matters, please see here: https://nakasaki-law.com/wp-content/uploads/2020/03/Japan-AML-CFT-and-FATF-recommendations.pdf.

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

Yes. The report for the 2008 review can be found at http://www.fatf-gafi.org/documents/documents/mutualevaluation-ofjapan.html. The report for the mutual evaluation conducted in 2019 is expected to be publicised after the discussion at the FATF plenary, which is expected to be held in June 2020. This may be prolonged due to the coronavirus pandemic.

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

Laws, regulations and guidance can be found on the government website of Japan: https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0100/.

The English translation of Japanese laws in general can be found on the below website of the government. However, some laws or their most current versions are not yet translated – see: http://www.japaneselawtranslation.go.jp/?re=02.

The AML Act was on the above website, but has since been amended and is no longer available.

Translations of the AML Act and Enforcement Ordinance of the AML Act pre-amendment can be found at the below websites of the NPA:

- https://www.npa.go.jp/laws/shokanhourei/hansyuu.pdf.
- https://www.npa.go.jp/sosikihanzai/jafic/en/hourei_e/data/sekoukisoku2504.pdf.

**Ryu Nakasaki** specialises in the areas of (i) finance (money transfer, loan, card business, AML, Fintech, etc.), and (ii) internet businesses (advertisement, data business, internet mall, online games, PII, IP, etc.). He assists clients in business collaboration agreements, licence agreements, and other transactions in the above areas and gives legal advice on regulations in Japan.
He is the author of "The Act on Prohibition of Criminal Proceeds and the Act of Foreign Exchange and Foreign Trade Act" which covers AML/CFT regulations, and of "Instalment Sales Act" which covers credit card-related regulations.
Mr. Nakasaki has engaged in (i) the amendment of the credit card act (or the Instalment Sales Act), and (ii) the supervision of related regulations including AML as a deputy director in the Japanese government.
Mr. Nakasaki lived in the U.S. for eight years.

**Nakasaki Law Firm**
1-9-7, Kudankita, Chiyodaku
Tokyo 102-0073
Japan

Tel: +81 3 6261 7500
Email: ryu@nakasaki-law.com
URL: www.nakasaki-law.com/en

**Kei Nakamura** is an attorney at law (Japan), and works in the areas of finance (card business, AML, Fintech, etc.). He assists clients in licence agreements, loan agreements and other transactions in the above areas and gives legal advice on regulations in Japan.
Mr. Nakamura studied at the University of Washington (Seattle).

**Nakasaki Law Firm**
1-9-7, Kudankita, Chiyodaku
Tokyo 102-0073
Japan

Tel: +81 3 6261 7500
Email: k-nakamura@nakasaki-law.com
URL: www.nakasaki-law.com/en

Nakasaki Law Firm was founded in 2018 and advises many clients, including financial institutions (banks, credit card companies, insurance companies, Fintech companies) as well as internet business companies on various Japan-related laws, issues and transactions.

**www.nakasaki-law.com/en**

Nakasaki & Sato Law Firm

# Liechtenstein


Laura Negele-Vogt, MLaw


Dr. Stefan Wenaweser, LL.M.

Marxer & Partner Attorneys at Law

## 1 The Crime of Money Laundering and Criminal Enforcement

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

The crime of money laundering, like almost all other criminal offences (except some minor misdemeanours which are only prosecuted upon request by the injured private party), is prosecuted by the Liechtenstein public prosecutor's office.

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

The Liechtenstein Criminal Code (hereinafter: StGB) distinguishes between money laundering with respect to assets originating from a criminal offence (§ 165 (1) and (2) StGB) and money laundering with respect to assets belonging to a criminal organisation or a terrorist group (§ 165 (3) StGB).

For a conviction pursuant to § 165 (1) or (2) StGB, the public prosecutor's office must prove that the perpetrator committed one of the punishable acts listed in § 165 (1) StGB (hiding, concealing the origin, providing false information in legal transactions with regard to the origin/true nature/ownership/location) or § 165 (2) StGB (appropriating, taking into safekeeping, investing, managing, converting, realising, transferring to a third party) with respect to assets originating from one of the predicate offences exhaustively enumerated in the law. In this regard, the law explicitly provides that it is also possible to commit the crime of money laundering with respect to expenses saved by a tax offence. Furthermore, the public prosecutor's office must prove that the perpetrator acted with intent ("*dolus eventualis*"), meaning that the perpetrator at least seriously considered the assets to be possibly originating from a crime and accepted this fact. If the predicate offence in question is tax fraud (Art. 140 of the Tax Act), "*dolus eventualis*" is not sufficient within the scope of § 165 (2) StGB. Instead, the public prosecutor's office has to prove that the perpetrator knew that the assets concerned originate from tax fraud.

According to Liechtenstein law, predicate offences are all offences with a minimum penalty of one year of imprisonment and the following misdemeanours: forgery of documents (§§ 223 StGB); suppression of documents (§ 229 StGB); false testimony before an administrative authority (§ 289 StGB); falsification of a piece of evidence (§ 293 StGB); suppression of a piece of evidence (§ 295 StGB); illegal residence (Art. 83 of the Foreigners Act); furtherance of illegal residence/entry (Art. 84 of the Foreigners Act); production or use of false identity papers or illegal use or transfer of authentic identity papers (Art. 85 of the Foreigners Act); all misdemeanours according to the Narcotics Act; tax fraud (Art. 140 of the Tax Act); and tax fraud and qualified tax evasion with respect to value-added tax (Art. 88 f of the Value Added Tax Act). Finally, an infraction pursuant to Art. 24 of the Market Abuse Act (market manipulation) can be a predicate offence. Ordinary tax evasion is not a predicate offence.

For a conviction pursuant to § 165 (3) StGB, the public prosecutor's office must prove that the perpetrator appropriated or took into safekeeping assets of a criminal organisation or a terrorist group on behalf of or in the interest of a criminal organisation or terrorist group. Furthermore, it must prove that the perpetrator acted with intent ("*dolus eventualis*").

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

The Liechtenstein Criminal Code is applicable and Liechtenstein law enforcement authorities are competent if either the predicate offence (*cf.* § 64 (1) (9) StGB) or the punishable act constituting money laundering (i.e. the concealing, the management … *cf.* § 62 StGB) was committed in Liechtenstein. In the latter case, it is irrelevant where the predicate offence was committed. Furthermore, it is noticeable that proceeds of foreign crimes which are not subject to the jurisdiction of Liechtenstein can be forfeited and confiscated if only the crime is punishable according to the law of the state in which the crime was committed (*cf.* § 65a StGB).

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

In principle, the public prosecutor's office is responsible for investigating and prosecuting money-laundering criminal offences. The public prosecutor's office may, however, instruct the police or the investigating judge to conduct measures of investigation (e.g. interrogations, assets transfer analysis, etc.). The police are also entitled to conduct measures by their own if they become aware of a suspicion that a criminal offence was committed. If, however, the suspicion concerns a serious offence or an offence which raises particular public interest, the public prosecutor's office has to be informed immediately. In any event, the police must inform the public prosecutor's office at the latest three months after the first investigation measure against a specific person was taken.

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

The Liechtenstein Criminal Code provides in general for corporate criminal liability and not only with respect to specific criminal offences. The law distinguishes between underlying acts committed by managers and underlying acts committed by "ordinary" employees. According to § 74a (1) StGB, legal entities are liable for any misdemeanours and crimes committed unlawfully and culpably by managers in the performance of business activities and within the framework of the purpose of the legal entity (except if the managers are acting in enforcement of the laws). In contrast, according to § 74a (3) StGB, legal entities are only liable for misdemeanours and crimes committed unlawfully (but not necessarily culpably) by "ordinary" employees if the act was made possible or was significantly facilitated by the failure of the managing staff to take the necessary and responsible measures to prevent such misdemeanours or crimes.

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

The Liechtenstein Criminal Code provides for different penalties depending on the specific act of money laundering committed (active concealing of the proceeds of crimes according to § 165 (1) StGB *vs.* commonplace activities such as a simple storage of the proceeds of crimes according to § 165 (2) StGB) and depending on the amount of assets laundered.

If the crime of money laundering is committed with respect to an amount exceeding CHF 75,000, the penalty provided for by law for an individual is between one and 10 years of imprisonment irrespective of the specific act committed. For legal entities, the maximum penalty in these circumstances is a monetary penalty of CHF 1,950,000 (up to 130 daily penalty units of a maximum of CHF 15,000). The same maximum penalties apply if the crime of money laundering was committed by a member of a criminal group that has been formed for the purpose of continued money laundering.

If the amount of assets concerned by the crime of money laundering does not exceed the threshold of CHF 75,000 and the crime of money laundering was not committed by a member of a criminal group, the penalty is up to three years of imprisonment (active concealing of the proceeds of crimes), and respectively, up to two years of imprisonment (commonplace activities such as a simple storage of the proceeds of the crimes) for individuals. For legal entities, the maximum penalty is, in these circumstances, a monetary penalty of CHF 1,275,000 (up to 85 daily penalty units of a maximum of CHF 15,000), and respectively, CHF 1,050,000 (up to 70 daily penalty units of a maximum of CHF 15,000).

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

According to § 57 (3) StGB, the statute of limitations for money laundering crimes is in general five years. In cases in which the threshold of CHF 75,000 is exceeded or the crime of money laundering was committed by a member of a criminal group, the statute of limitations is 10 years. However, if, during the limitation period, the perpetrator commits another offence that arises from the same harmful inclination, the limitation period is prolonged until the limitation period has also expired for the second offence.

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

Liechtenstein has only two electoral districts, but no provinces. Therefore, there is only enforcement at national level.

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

In Liechtenstein, there are no special forfeiture or confiscation authorities. It is up to the Liechtenstein prosecutor's office to ask the criminal court for a forfeiture or confiscation.

Any property used or intended to be used to commit an intentional criminal offence, as well as all goods originating from committing an intentional criminal offence, can be confiscated if, at the time of the decision of the criminal court (first instance), the perpetrator is the sole owner (*cf.* § 19a StGB). Furthermore, substitute values of such goods which are in the sole ownership of the perpetrator at the time of the decision of the criminal court (first instance) can be confiscated.

Furthermore, pursuant to § 20 (1) and (2) StGB, all assets received for committing a punishable act as well as all assets obtained through a punishable act, including their profits and substitute values, can be forfeited. If the assets subject to forfeiture according to § 20 (1) and (2) StGB are no longer present or a forfeiture is impossible for other grounds, the criminal court may forfeit an amount of money equivalent to these assets (*cf.* § 20 (3) StGB). In addition, the criminal court may also forfeit the amount of money the perpetrator has saved in expenses by committing the punishable act.

§ 20a StGB provides for certain exceptions in which a forfeiture is excluded despite the fact that the conditions according to § 20 StGB are met. In particular, forfeiture is excluded when a third party who has acquired the concerned assets in return for payment without knowing about the punishable act is involved.

Pursuant to § 20b StGB, it is also possible to forfeit assets which are under the control of a criminal organisation or a terrorist group or which have been provided or collected for the financing of terrorism (so-called "extended forfeiture"). If a crime (any criminal offence with a maximum penalty of more than three years of imprisonment) has been committed, for which or by which assets have been obtained, any other assets obtained in a temporal connection with the crime committed are subject to forfeiture if there is reason to believe that they were derived from an unlawful act and if their lawful origin cannot be credibly shown. If one of the following misdemeanours (money laundering, criminal association, terrorist offence or active/passive bribery) has been committed in a continuous or repeated manner for which or by which assets have been obtained, any other assets obtained in a temporal connection with these acts shall also be subject to forfeiture if there is reason to believe that they were derived from further misdemeanours of this kind and if their lawful origin cannot be credibly shown.

Finally, pursuant to § 26 StGB, all objects used by the perpetrator or intended by the perpetrator to be used to commit the punishable act and all objects obtained from the punishable act are subject to a deprivation order if these objects endanger the safety of persons, morality or the public order.

A forfeiture (§ 20 StGB), an extended forfeiture (§ 20b StGB) or a deprivation (§ 26 StGB) is also possible if there has been no criminal conviction. If the public prosecutor believes that

there are sufficient reasons to assume that the preconditions for forfeiture, extended forfeiture or deprivation are met and it is not possible to decide on this in criminal proceedings, the prosecutor can submit a separate application for the issuing of such pecuniary order.

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

Based on the publicly available information, no convictions of banks or other regulated financial institutions have occurred. However, it is publicly known that a (former) vice director of a bank and other employees of banks, respectively, regulated financial institutions who have been convicted of other crimes such as fraud or embezzlement have also been convicted of laundering the proceeds of their own crimes.

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

The Liechtenstein Criminal Procedure Code (hereinafter: StPO) does not provide for the opportunity to conclude settlements between the public prosecutor's office and a perpetrator. Thus, in general, criminal actions are only resolved through the judicial process. However, the public prosecutor's office can, under certain circumstances, refrain from filing charges against a perpetrator even though it realises sufficient grounds of suspicion.

According to §§ 22a ff StPO, the public prosecutor shall withdraw from the prosecution of a punishable act if, in view of the payment of an amount of money, the performance of community service, the setting of a probation period or a victim-offender mediation, punishment does not seem advisable as a means to prevent the suspect from committing punishable acts or for counteracting the commission of punishable acts by others. In addition, the withdrawal from prosecution requires that (i) the punishable act constitutes an offence explicitly listed in § 22a (2) StPO, (ii) the suspect's level of culpability would not have to be considered grave, and (iii) the offence has not caused the death of a human being. With respect to money laundering, a withdrawal from the prosecution according to §§ 22a ff StPO is only possible if the threshold of CHF 75,000 is not exceeded and the crime was not committed by a member of a criminal group.

Such withdrawals from the prosecution are not public.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

It is the Liechtenstein legislative authority (i.e. the Liechtenstein parliament called "Landtag" and the prince who must approve every law passed by parliament) who imposes anti-money laundering requirements on financial institutions and other businesses. It has done so by enacting the Due Diligence Act (hereinafter: SPG). The Liechtenstein Government has specified some of the anti-money laundering requirements already provided for by the SPG in the Due Diligence Ordinance (hereinafter: SPV). Finally, the Liechtenstein Financial Market Authority and the Liechtenstein FIU have issued guidelines, communications and instructions with respect to anti-money laundering requirements.

For the details of these anti-money laundering requirements, please see the responses to section 3 (in particular question 3.1).

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

The Liechtenstein Bankers Association has issued guidelines on due diligence obligations of banks in dealing with foreign correspondent banks and with regard to their customers' tax compliance.

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

The Liechtenstein Chamber of Lawyers is the only professional association which is responsible for anti-money laundering compliance and enforcement against their members. With respect to all other financial institutions and businesses subject to due diligence requirements, the Liechtenstein Financial Market Authority (hereinafter: FMA) is responsible for anti-money laundering compliance and enforcement.

**2.4 Are there requirements only at national level?**

As Liechtenstein is a small state, there are only requirements at national level.

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

The FMA is responsible for compliance with and enforcement of anti-money laundering requirements (with the exception of lawyers, for which the Liechtenstein Chamber of Lawyers is solely competent). The FMA, as well as the FIU (with respect to suspicious transaction reports), have issued guidelines which show how they construe the provisions of the SPG and the SPV in practice. Furthermore, the FMA publishes an annual report about its activity, as well as a brochure called "FMA-Praxis" once a year, in which it informs about its own relevant decisions, relevant decisions of the FMA Complaints Commission, relevant decisions of the administrative court and relevant decisions of the constitutional court in anonymised form.

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

Yes, there is. The Liechtenstein FIU is competent for analysing any suspicious transaction report received by a financial institution or other business subject to due diligence requirements. In the event of a reasonable suspicion of money laundering, predicate offences to money laundering, organised crime or terrorist financing, it has to file a report with the Liechtenstein public

prosecutor's office containing the analysis and any other additional relevant information. The report to the Liechtenstein public prosecutor's office may not contain any details about the source of the information or disclosure.

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

With respect to penalties, the limitation period is three years. For all other supervisory measures, the law does not provide for an explicit limitation period.

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

The maximum penalties for failure to comply with anti-money laundering requirements are six months of imprisonment or a monetary penalty of up to CHF 360,000 (up to 360 daily penalty units of a maximum of CHF 1,000), or a fine of up to CHF 200,000 for administrative infractions which are prosecuted and judged by the FMA and not by the public prosecutor's office and the criminal court. In case of serious, repeated or systematic violations, the fine for administrative infractions can be raised up to CHF 5,000,000, or up to 10% of the annual total turnover (whichever amount is higher). For some of the businesses subject to due diligence obligations, the maximum fine is CHF 1,000,000, or double the amount gained through the administrative infraction (whichever amount is higher).

Subject to penalty are any failures with respect to suspicious transaction reports (i.e. violating the reporting requirement, carrying out suspicious transactions before filing the report or carrying out suspicious transactions without ensuring the paper trail, informing third parties about the suspicious transactions reports and not freezing assets in case of a suspicion of terrorist financing). Furthermore, it constitutes a criminal infringement to either not provide the FIU with information requested according to the law, or to provide them with false information.

Almost every intentional failure of anti-money laundering obligations provided for by the SPG constitutes an administrative infraction (the list in the SPG is more than two pages long).

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

The supervisory authorities may prohibit the commencement of new business relationships for a limited period of time and they may request the competent authority to undertake appropriate disciplinary measures. Furthermore, in the event of repeated, systematic or serious violations, the supervising authorities may: (i) publicly disclose decisions against a financial institution or business subject to due diligence requirements (including the name of the infringer); (ii) temporarily prohibit the performance of the activity it has authorised under special legislation; (iii) withdraw the licence it has granted under special legislation; or (iv) temporarily prohibit members of the executive body and other natural persons from performing the executive functions it has authorised or taking up such functions yet to be authorised.

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

The penalties are not only administrative. All violations of requirements with respect to suspicious transaction reports constitute criminal misdemeanours or criminal infractions which fall in the competence of the criminal court.

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

When imposing the penalties, the criminal court, respectively, the supervisory authorities, must take into account the principle of proportionality and the principle of efficiency. Decisions of the criminal court can be appealed within 14 days to the court of appeal (the StPO applies). Decisions of the FMA can be appealed within 14 days to the FMA Complaints Commission and afterwards to the administrative court. Decisions of the Liechtenstein Chamber of Lawyers can only be appealed to the administrative court. Final decisions by the FMA or the Liechtenstein Chamber of Lawyers, as well as final decisions by the criminal court, constitute executory titles which can be enforced.

Pursuant to Liechtenstein law, not all decisions taken by the FMA (or the criminal court) are public. The decisions of the FMA are only published in case of serious, systematic or repeated violations. But even in this case, the FMA may refrain from publication or only publish the decisions in anonymised form, e.g., for reasons of proportionality. Having said that, the FMA informs about its activities and decisions in annual reports and in brochures ("FMA-Praxis") in anonymised form. Decisions of the criminal court are only made public if considered relevant by the courts.

Yes, it is publicly known that penalty decisions (at least of criminal courts) have been appealed by financial institutions.

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

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

The following persons are subject to due diligence (e.g. anti-money laundering requirements):

- banks and investment firms;
- e-money businesses;
- undertakings for collective investment that market their unit certificates or units;
- insurance undertakings;
- the *Liechtensteinische Post Aktiengesellschaft*, insofar as it pursues activities beyond its postal service that must be reported to the FMA;
- exchange offices (including Trustworthy Technology (TT) exchange service providers);

- insurance brokers;
- payment service providers;
- asset management companies;
- service profilers for legal entities;
- casinos and providers of online gaming;
- lawyers and law firms (insofar as they provide tax advice or assist in the planning and execution of financial or real estate transactions);
- members of tax consultancy professions and external bookkeepers;
- real estate agents;
- persons trading in goods, insofar as payment is made in cash and the amount involved is CHF 10,000 or more, irrespective of whether the transaction is executed in a single operation or in several operations which appear connected;
- TT services providers who are subject to registration according to the Token and TT Service Provider Act;
- token issuers with domicile in Liechtenstein who are not subject to registration according to the Token and TT Service Provider Act and who issue tokens in their own name or non-professionally in the name of their principal, insofar as they handle transactions above the amount of CHF 1,000; and
- operators of trading platforms for virtual currencies.

Such persons shall perform the following duties taking a risk-based approach:

- identification and verification of the identity of the contracting party;
- identification and verification of the identity of the beneficial owner;
- identification and verification of the identity of the recipient of distributions from legal entities established on a discretionary basis and the beneficiary of life assurance policies and other insurances with investment-related objectives;
- establishment of a business profile; and
- supervision of business relationships at a level that is commensurate with the risk.

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

As stated above, TT services providers subject to registration according to the Token and TT Service Provider Act, token issuers with domicile in Liechtenstein who issue tokens in their own name or non-professionally in the name of their principal, operators of trading platforms for virtual currencies and TT exchange service providers are, in principal, subject to due diligence.

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

TT services providers who are subject to registration according to the Token and TT Service Provider Act are obliged to use IT-based systems to control the history of the virtual currencies respective of the tokens in the TT-system with a risk-based approach. All other financial institutions and designated businesses should use IT-based systems to supervise business relationships with a risk-based approach, if this is possible, and if the costs are in an adequate relation to the intended objectives. The IT-based system used shall be suitable and in accordance with the technical possibilities.

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

The persons subject to due diligence shall keep a record of compliance with the duties of due diligence and the reporting requirements as provided in the SPG.

Such persons shall establish and maintain due diligence files. In these files, client-related documents, business correspondence and vouchers are to be retained for 10 years from the end of the business relationship and/or from the execution of an occasional transaction, whereas transaction-related documents, business correspondence and vouchers shall be retained for 10 years from conclusion of the transaction and/or from their issue.

There is no reporting requirement in relation to a threshold. However, any suspicion in relation to money laundering has to be reported immediately (see also the answer to question 3.9).

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

No, see above the answer to question 3.4.

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

Yes, the cross-border transactions reporting requirements apply to all financial intermediaries operating across borders.

Reporting has to be done in connection with legal and reputational risks arising from cross-border business activities. The FMA has to be informed in cases of substantial significance.

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

When embarking upon a business relationship or concluding an occasional transaction, the person subject to due diligence shall establish the identity of the contracting party and verify that identity by consulting a supporting document (original or certified copy) relating to the contracting party and obtaining and recording the following details:

a) for natural persons: last name; first name; date of birth; residential address; state of residence and nationality; and
b) for legal entities: name or company type; legal form; address of registered office; state of domicile; date established; place and date of entry in the Commercial Register, where applicable; and the names of the bodies or trustees acting formally on behalf of the legal entity in the relationship with the person subject to due diligence.

With regard to business relationships and transactions with politically exposed persons, enhanced due diligence requirements have to be applied.

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

Correspondent bank relationships with shell banks are prohibited according to the SPG.

**3.9 What is the criteria for reporting suspicious activity?**

Where suspicion of money laundering, a predicate offence to money laundering, organised crime, or terrorist financing exists, the persons subject to due diligence must immediately report to the FIU in writing.

The person subject to due diligence shall verify the plausibility of each customer statement to the best of its ability. If investigations reveal that the transactions or circumstances are implausible, this will trigger the reporting requirement.

The indicators of money laundering, organised crime and financing of terrorism are listed in Annex 3 of the SPV.

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

Yes, in Liechtenstein a commercial register exists, which is open to the public and constitutes conclusive evidence. Moreover, on 1 August 2019, a new law which provides for a register of the beneficial owners of domestic legal entities entered into force. The Office of Justice may provide information contained in the latter register to persons subject to due diligence upon their request. Other third parties have to show a legitimate interest in the field of combatting money laundering, predicated offences of money laundering and terrorist financing.

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

The payment order contains the name, account number and address of the payer as well as the name and account number of the beneficiary.

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

It is only permitted if a custodian has been appointed and the issued bearer shares are deposited with the custodian. The custodian must be entered in the commercial register stating his function. The custodian has to keep a register in which each bearer, who has to be identified by the custodian in accordance with the law (Art. 326c PGR), is entered. The person entered into the register is considered as shareholder. The result of the legal provisions is that the bearer is identified and documented in accordance with the rules of the due diligence legislation (SPG).

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

No – the financial institutions and other businesses that are subject to anti-money laundering requirements are mentioned under question 3.1.

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

The SPG applies to various business sectors and, in particular, also applies to persons trading in goods (see question 3.1 above). However, there are no requirements in relation to free trade zones, because in Liechtenstein there are no free trade zones or other special geographic areas.

## 4 General

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

Different legislative changes to implement Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, have been proposed by the Liechtenstein Government. It is unclear when the Liechtenstein Parliament will discuss these proposals.

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

According to the last evaluation report by Moneyval (dated 2 April 2014), the legal framework as such is closely in line with the FATF recommendations. However, the effective implementation was criticised. In particular, the fact that there was only one conviction of money laundering in the period between 2007 and 2014 was criticised.

Following the release of this evaluation report, Liechtenstein has undertaken several changes in legislation to facilitate enforcement of the anti-money laundering regime. In the period from 2014 to 2018, there have been 27 final convictions of money laundering. As the next evaluation by Moneyval will not take place before 2021, it is not clear how the different changes in legislation are assessed by independent organisations.

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

Yes, the last on-site visit by Moneyval was in June 2013.

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

The relevant anti-money launderings laws are publicly available on http://www.gesetze.li (only in German) or – alternatively – on http://www.fma-li.li. The FMA provides English translations of the most relevant laws. They are, unfortunately, not always up to date. The FMA also publishes its guidelines, instructions and communications on its website (a few of them in English).

Criminal court decisions are available on http://www.gerichtsentscheidungen.li (in German only). The FMA publicly informs about its activity and its decisions in annual reports (available in English and in German) and "FMA-Praxis" brochures (available only in German).

**Laura Negele-Vogt, MLaw**, born in 1990, studied law at the University of Lucerne and Northwestern Pritzker School of Law (student exchange programme). She joined Marxer & Partner Attorneys at Law in 2014 and passed the Bar exam in 2017. She is part of the litigation team at Marxer & Partner Attorneys at Law.

**Marxer & Partner Attorneys at Law**
Heiligkreuz 6, Postfach 484
LI-9490 Vaduz
Liechtenstein

Tel: +423 235 81 81
Email: laura.negele@marxerpartner.com
URL: www.marxerpartner.com

**Dr. Stefan Wenaweser, LL.M.**, born in 1972, studied law at the University of Innsbruck, the University of Paris Val-de-Marne and the University of Edinburgh. He received an LL.M. from King's College London and a *Dr. iur.* degree from the University of Innsbruck. He has practised law since 2000, passed the Bar exam in 2003 and became a partner of Marxer & Partner in 2008. He specialised in the law of trusts and company law during his studies, and in his practice he regularly advises clients in foundation law, trust law and litigation. Moreover, he is a specialist in the defence of white-collar crime cases and legal assistance in criminal matters.
Stefan frequently speaks at conferences and regularly contributes to renowned publications on trust law, wealth and estate planning, litigation and white-collar crime. In addition, he functions as a member of the board of the Liechtenstein Institute of Professional Trustees and Fiduciaries.

**Marxer & Partner Attorneys at Law**
Heiligkreuz 6, Postfach 484
LI-9490 Vaduz
Liechtenstein

Tel: +423 235 81 81
Email: stefan.wenaweser@marxerpartner.com
URL: www.marxerpartner.com

Marxer & Partner Attorneys at Law was very much involved in shaping Liechtenstein as a financial centre and has been growing with it. Established in 1925, it is the oldest and largest law firm in Liechtenstein, with 13 partners, four of counsels, 10 associates and a supporting staff of about 50 paralegals and administrative specialists. Of all firms providing legal services to a demanding international clientele, Marxer & Partner has certainly become the most renowned in Liechtenstein.
For many years Marxer & Partner has focused its activities on the fields of corporate law, M&A, trust and estate planning, and capital markets, as well as tax. The firm provides in-depth knowledge and excellent advice in these fields to its international client base. Together with its auxiliary trust, management and auditing companies, Marxer & Partner forms a centre of excellence that can handle all sorts of issues in financial, legal, tax, business management, and real estate affairs.
The firm represents Liechtenstein exclusively at Lex Mundi, the worldwide association of independent law firms.

**www.marxerpartner.com**

MARXER & PARTNER
RECHTSANWÄLTE

# Malaysia

Rahmat Lim & Partners

Karen Foong Yee Ling

## 1 The Crime of Money Laundering and Criminal Enforcement

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

The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "**AMLATFA**") is the primary Malaysian statute dealing with anti-money laundering and anti-terrorism financing. The AMLATFA is federal legislation that has application throughout all the States and federal territories of Malaysia.

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

**Offence of money laundering**

Section 4 of the AMLATFA stipulates that any person who:

(a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;
(b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence;
(c) removes from or brings into Malaysia proceeds of an unlawful activity or instrumentalities of an offence; or
(d) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence,

commits a money laundering offence.

**Predicate offences**

Generally, the terms "proceeds of an unlawful activity" and "instrumentalities of an offence" refer to proceeds or dealings derived or connected with "unlawful activity".

The term "unlawful activity" means:

(a) any activity which constitutes any serious offence or any foreign serious offence; or
(b) an activity which is of such nature, or occurs in such circumstances, that it results in or leads to the commission of any serious offence or any foreign serious offence,

regardless of whether such activity, wholly or partly, takes place within or outside Malaysia.

"Serious offences" mean:

(a) any of the offences specified in the Second Schedule of the AMLATFA;
(b) an attempt to commit any of those offences; or
(c) the abetment of any of those offences.

In addition, the AMLATFA defines "foreign serious offence" as an offence:

(a) against the law of a foreign State stated in a certificate purporting to be issued by or on behalf of the government of that foreign State; and
(b) that consists of or includes an act or activity which, if it had occurred in Malaysia, would have constituted a serious offence.

**Tax evasion**

Tax evasion constitutes one of the offences under the Second Schedule of the AMLAFTA and is accordingly one of the predicate offences for money laundering.

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

Yes. Under the AMLATFA, any offence under the AMLATFA by, *inter alia*:

(a) any citizen or permanent resident in any place outside and beyond the limits of Malaysia;
(b) any person against a citizen of Malaysia; or
(c) any person who after the commission of the offence is present in Malaysia,

may be dealt with as if it had been committed at any place within Malaysia.

Money laundering of the proceeds of foreign crimes is punishable. Please refer to the definition of foreign serious offences in question 1.2 above.

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

Depending on the nature of the crime, the investigation of offences under the AMLATFA may be conducted by various enforcement agencies including the Royal Malaysia Police or the competent authority appointed pursuant to the AMLATFA to implement the provisions of the AMLATFA, the Central Bank of Malaysia, Bank Negara Malaysia ("**BNM**"). As the financial services regulator, BNM is empowered to investigate money laundering cases relating to the laws administered by BNM such as the Financial Services Act 2013 and the Islamic Financial Services Act 2013.

No prosecution for an offence under the AMLATFA may be instituted except with the written consent of the Attorney General of Malaysia in his capacity as Public Prosecutor.

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

Criminal liability in respect of offences under the AMLATFA extends to both corporates and natural persons. By virtue of sections 2 and 3 of the Interpretation Acts 1948 and 1967, the term "person" under the AMLATFA includes a body of persons, corporate or unincorporated.

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

Different offences under the AMLATFA have different maximum penalties. The maximum penalty for a money laundering offence under section 4 of the AMLATFA is imprisonment for 15 years and a fine of not less than five times the sum or value of the proceeds of the unlawful activity or instrumentalities of the offence at the time the offence was committed or RM5 million, whichever is higher.

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

There is no statutory time limit for prosecution of money laundering offences under the AMLATFA.

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

There are no parallel state or provincial criminal offences for money laundering. Enforcement is only at national level.

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

There is no separate forfeiture or confiscation regime apart from that set out under the AMLATFA in relation to money laundering offences.

In any prosecution for a money laundering offence under section 4 of the AMLATFA or a terrorism financing offence, the court will make an order for the forfeiture of any property which is proved to be:

- the subject matter or evidence relating to the commission of such offence;
- terrorist property;
- the proceeds of an unlawful activity; or
- the instrumentalities of an offence,

where:

(i) the offence is proved against the accused; or

(ii) the offence is not proved against the accused but the court is satisfied that:

(ia) the accused is not the true and lawful owner of such property; and

(ib) no other person is entitled to the property as a purchaser in good faith for valuable consideration.

Where in respect of any property seized under the AMLATFA, there is no prosecution or conviction under section 4 or a terrorism financing offence, the Public Prosecutor may, before the expiration of 12 months from the date of the seizure, or where there is a freezing order, 12 months from the date of the freezing, apply to a judge of the High Court for an order of forfeiture of that property if he is satisfied that such property is:

- the subject matter or evidence relating to the commission of such offence;
- terrorist property;
- the proceeds of an unlawful activity; or
- the instrumentalities of an offence.

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

We have not identified any cases in which financial institutions or their directors, officers or employees have been convicted of money laundering under the AMLATFA, although we are aware that charges have been brought against former bank employees for money laundering.

In 2015, BNM imposed an administrative fine of RM53.7 million on AMMB Holdings Bhd (Ambank Group). Whilst the exact reasons for the fine have not been disclosed, it was announced that the fine had been imposed as a result of non-compliance with anti-money laundering and counter-terrorism financing obligations under the Financial Services Act 2013 and the Islamic Financial Services Act 2013.

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

Criminal actions are resolved through the judicial process. Malaysian judgments are publicly available online.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

The principal anti-money laundering requirements are contained in the AMLATFA. The AMLATFA makes it an offence for any person to engage in or abet the commission of money laundering and terrorist financing, and seeks among other things, to implement measures for the prevention of money laundering and terrorism financing offences. These measures include the imposition of obligations on reporting institutions (as described in the First Schedule of the AMLATFA) for reporting of transactions exceeding a specified threshold, and suspicious transactions, as well as customer due diligence.

The reporting institutions under the AMLATFA include, *inter alia*, banks and insurers as well as professionals such as advocates and solicitors.

BNM as the competent authority appointed under the AMLATFA is empowered to issue to reporting institutions guidelines, circulars or notices to give full effect to or for carrying out the provisions of the AMLATFA. In this regard,

BNM has issued various guidelines to reporting institutions based on the industry sector including, *inter alia*:

(i) Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) ("**Policy Document for Financial Institutions**") applicable to financial institutions such as banks, insurers, money services businesses and issuers of designated payment instruments;

(ii) Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions & Non-Bank Financial Institutions (AML/CFT and TFS for DNFBPs and NBFIs) ("**Policy Document for Non-Financial Businesses, Institutions and Professions**") applicable to businesses and professions such as advocates and solicitors, casinos, accountants and company secretaries; and

(iii) The Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6) ("**Policy Document for Digital Currencies**").

Additionally, the Labuan Financial Services Authority has sectoral guidelines applicable to Labuan entities relating to sectors such as banking, insurance and takaful, trust company and capital market and other business sectors. The Securities Commission has issued guidelines on prevention of money laundering and terrorism financing for capital market intermediaries under its purview.

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

Yes, there are anti-money laundering requirements imposed by self-regulatory organisations and professional associations, including the Bar Council of Malaysia (advocates and solicitors practising in West Malaysia) and the Malaysia Institute of Accountants (professional accountants).

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

Failure to comply with the circulars or guidelines issued by the relevant self-regulatory organisations or professional associations may result in disciplinary actions against the members.

### 2.4 Are there requirements only at national level?

These requirements are only applicable at the national level.

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

BNM, as the competent authority, as well as the relevant supervisory authority of a reporting institution, is responsible for examination for compliance and enforcement of anti-money laundering requirements. Under section 21 of the AMLATFA, the relevant supervisory authority of a reporting institution may, *inter alia*, examine and supervise reporting institutions, and regulate and verify, through regular examinations, that a reporting institution adopts and implements compliance programmes to guard against and detect any offence under the AMLAFTA. The policy documents and guidelines issued by BNM and supervisory authorities such as the Labuan Financial Services Authority and the Securities Commission are publicly available on their websites. Please refer to question 2.1 above.

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

Yes, the Financial Intelligence Unit ("**FIU**"), established within the Financial Intelligence and Enforcement Department in BNM, manages and provides comprehensive analysis of the financial intelligence received relating to money laundering and terrorism financing.

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

There is no statutory time limit for competent authorities to bring enforcement actions.

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

Under section 22 of the AMLATFA, the maximum penalty for failure by a reporting institution to ensure the reporting institution's compliance with its obligations under Part IV (Reporting Obligations) of the AMLATFA is a fine not exceeding RM1 million or imprisonment for a term not exceeding three years or both. In the case of a continuing offence, there will be an additional fine not exceeding RM3,000 for each day or part thereof during which the offence continues to be committed.

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

In minor cases of non-compliance, BNM or the relevant supervisory authority may issue a warning letter to the relevant reporting institution.

Under the AMLATFA, BNM may, upon application to the court and satisfying the court that a reporting institution has failed without reasonable excuse to comply with any obligations under the AMLATFA, obtain an order against the officers or employees of that reporting institution on such terms as the court deems necessary to enforce compliance with such obligations. Notwithstanding this, BNM may also direct or enter into an agreement with any reporting institution to implement any action plan to ensure compliance with its obligations under Part IV (Reporting Obligations) of the AMLATFA.

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

Yes, violations of anti-money laundering obligations are also subject to criminal sanctions including imprisonment and fines.

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

The process for assessment and collection of sanctions is dependent on the relevant competent authority or enforcement agency. Details of sanctions imposed are not always made publicly available – these could include, for example, supervisory letters, reprimand/warning and administrative fines or penalties. Generally, administrative decisions or sanctions may be challenged by way of judicial review of the High Court. However, this option is rarely pursued in practice.

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

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

Reporting institutions under the AMLATFA are subject to anti-money laundering requirements including record-keeping, customer due diligence and reporting of suspicious transactions. The full list of reporting institutions can be found in the First Schedule of the AMLATFA.

These include, *inter alia*:

- activities carried out by a licensed bank, licensed investment bank, licensed insurer, approved financial adviser, approved insurance broker, approved issuer of designated payment instrument and approved money broker under the Financial Services Act 2013;
- activities carried out by a holder of a licence under the Capital Markets and Services Act 2007;
- activities carried out by an advocate and solicitor as defined in the Legal Profession Act 1967; and
- activities carried out by a member as defined in the Accountants Act 1967.

Please refer to question 2.1 above for a brief description of the obligations imposed on reporting institutions.

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

Under the First Schedule to the AMLATFA, a reporting institution includes any person who provides any or any combination of the following services:

- exchanging digital currency for money;
- exchanging money for digital currency; and/or
- exchanging one digital currency for another digital currency,

whether in the course of carrying on a digital currency exchange business or otherwise.

BNM has issued the Policy Document for Digital Currencies, which is applicable to such reporting institutions. Apart from the usual reporting obligations applicable to all reporting institutions relating to, for example, customer due diligence and record keeping, reporting institutions must declare their details to BNM in the form specified under the Policy Document for Digital Currencies.

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

Yes, under section 19 of the AMLATFA, a reporting institution is required to adopt, develop and implement internal programmes, policies, procedures and controls to guard against and detect any offence under the AMLAFTA. The programmes must include the establishment of procedures to ensure high standards of integrity of its employees and a system to evaluate the personal, employment and financial history of employees, ongoing employee training programmes to instruct employees with regard to their responsibilities specified under the AMLATFA, the appointment of compliance officers, and an independent audit function to check for compliance with such programmes.

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

A reporting institution must maintain any account, record, business correspondence and document relating to an account, business relationship, transaction or activity with a customer or any person as well as the results of any analysis undertaken, as the case may be, for a period of at least six years from the date the account is closed or the business relationship, transaction or activity is completed or terminated.

A reporting institution must keep a record of any transaction involving the domestic currency or any foreign currency exceeding such amount as BNM may specify, and must report to BNM any transaction exceeding such amount as BNM may specify.

Under a circular issued by BNM on 28 December 2018, the relevant threshold for making a cash threshold report ("**CTR**") is RM25,000 and above in a day. CTR obligations are imposed on banking institutions and licensed casinos. Such reporting institutions are required to submit a CTR to BNM in respect of any cash transaction exceeding RM25,000 and above in a day. This includes cash transactions involving physical currencies (domestic or foreign currency) and bearer negotiable instruments such as travellers' cheques but bank drafts, cheques, electronic transfers or fixed deposit rollovers or renewals are excluded. The requirements for making a CTR are applicable to single or multiple cash transactions within the relevant amount specified in a day, and where there are deposit and withdrawal transactions, the amounts must be aggregated and not offset against each other.

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

Apart from large cash transactions, reporting institutions must also file a Suspicious Transaction Report with the Financial Intelligence and Enforcement Department of BNM in respect of any transaction (attempted or proposed), regardless of the amount, where such transaction meets the criteria specified in question 3.9 below.

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

Travellers entering or leaving Malaysia with cash and/or negotiable bearer instruments (e.g. traveller's cheques, bearer cheques) exceeding an amount equivalent to US$10,000 must make a declaration.

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

Under the Policy Document for Financial Institutions issued by BNM applicable to financial institutions (e.g. licensed banks), the customer due diligence ("**CDD**") requirements to be undertaken by reporting institutions include:

- identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
- verifying that any person acting on behalf of the customer is so authorised, and identifying and verifying the identity of that person;
- identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and
- understanding, and, where relevant, obtaining information on, the purpose and intended nature of the business relationship.

Specific CDD measures are set out in the Policy Document for Financial Institutions in relation to documents and information to be obtained in relation to, for example, an individual customer and beneficial owner, legal persons, legal arrangements, and clubs, societies and charities.

Enhanced CDD is required to be performed where the money laundering/terrorism financing risk is assessed as higher risk; for example, upon determination that a customer or a beneficial owner is a foreign politically exposed person.

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

Yes, under the Policy Document for Financial Institutions issued by BNM applicable to licensed banks, reporting institutions must not establish or have any business relationship with shell banks.

**3.9 What is the criteria for reporting suspicious activity?**

A reporting institution must promptly report to BNM:

- any transaction where the identity of the person involved, the transaction itself or any other circumstances concerning that transaction gives any officer or employee of the reporting institution reasons to suspect that the transaction involves proceeds of an unlawful activity or instrumentalities of an offence; or
- any transaction or property where any officer or employee of the reporting institution has reason to suspect that the transaction or property involved is related or linked to, is used or is intended to be used for or by, any terrorist act, terrorist, terrorist group, terrorist entity or person who finances terrorism.

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

Yes. The Companies Commission of Malaysia ("**CCM**") maintains a public registry of companies, businesses and Limited Liability Partnerships ("**LLP**"). Reports containing information such as a company's profile, particulars of directors/officers, particulars of share capital, particulars of shareholder and company charges are publicly available online for purchase.

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

Yes, under the Policy Document for Financial Institutions issued by BNM applicable to licensed banks, accurate originator information pertaining to name, account number (or unique reference number if there is no account number) which permits traceability of the transaction, and address (or *in lieu* of address, date and place of birth) and beneficiary information pertaining to name and account number (or unique reference number if there is no account number) which permits traceability of the transaction, are required. This applies to reporting institutions which are ordering institutions for message or payment instructions for all cross-border wire transfers involving an amount equivalent to RM3,000 and above. Insofar as domestic wire transfers are concerned, the information accompanying the wire transfer should include the originator information as indicated for cross-border wire transfers (unless the information can be made available to the beneficiary institution and relevant authorities by other means).

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

No. Under the Companies Act 2016, a company is prohibited from issuing bearer shares.

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

Yes. BNM has issued the Policy Document for Non-Financial Businesses, Institutions and Professions to address the requirements for non-financial institution businesses. There are specific CDD requirements to be complied with by the following non-financial institution businesses:

- licensed casinos;
- licensed gaming outlets;
- lawyers, accountants and company secretaries;

- trust companies;
- dealers in precious metals or precious stones;
- registered estate agents;
- moneylenders; and
- pawnbrokers,

as set out under paragraph 14A to 14H of the Policy Document for Non-Financial Businesses, Institutions and Professions.

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

BNM has issued policy documents pertaining to various business sectors. Please see the response to question 2.1 above for the full list of the policy documents.

## 4 General

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

We are not aware of any material reforms being proposed at this stage.

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

A Mutual Evaluation Report dated September 2015 by the FATF is accessible here: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Malaysia-2015.pdf, and the 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating by the FATF dated October 2018 is accessible here: http://www.fatf-gafi.org/media/fatf/documents/reports/fur/FUR-Malaysia-2018.pdf.

Under the 2018 Report and in light of Malaysia's progress since the Mutual Evaluation Report was adopted, Malaysia's technical compliance with the FATF Recommendations has been re-rated and Malaysia is generally rated as "partially compliant", "compliant" and "largely compliant" in respect of the 40 FATF Recommendations. The FATF has continued to place Malaysia in "enhanced follow-up" on the basis that it had a moderate level of effectiveness for 7 of the 11 effectiveness outcomes (FATF Procedures, para. 79(a)(iii)). According to the enhanced follow-up process, Malaysia will continue to report back to the FATF on progress to strengthen its implementation of AML/CFT measures.

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

Yes, please see the response to question 4.2 above.

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

Yes, the materials are available in English.

The AMLATFA, sectoral policy documents issued by BNM and other circulars, guidance and technical notes can be accessed at BNM's AML/CFT website: http://amlcft.bnm.gov.my/AMLCFT07.html.

**Karen Foong Yee Ling** has experience in advising financial institutions and corporations on financial services laws and regulations. These include advising on licensing, regulatory, compliance and other conduct of business requirements for banking, securities, derivatives, asset management and other capital markets businesses.
She has also assisted domestic and foreign entities in relation to regulatory enquiries and investigations in connection with potential, alleged or actual breaches of laws or binding guidelines.
Karen graduated from the University of Reading with an LL.B. degree in 2008 and the University of Oxford with the Bachelor of Civil Law in 2011. She was admitted as an Advocate & Solicitor of the High Court of Malaya in 2010.

**Rahmat Lim & Partners**
Suite 33.01, Level 33, The Gardens North Tower
Mid Valley City, Lingkaran Syed Putra
59200 Kuala Lumpur
Malaysia

Tel: +603 2299 3903
Email: karen.foong@rahmatlim.com
URL: www.rahmatlim.com

Established in 2010 with slightly more than a dozen lawyers, Rahmat Lim & Partners has grown to become one of the largest corporate law firms in Malaysia. With over 90 lawyers in Kuala Lumpur, and as part of the Allen & Gledhill network, we handle a wide range of domestic and cross-border matters, including some of the most significant and complex transactions involving Malaysia. Our distinctive culture reflects the DNA which runs deep within the A&G network, as highlighted by our use of the same market-leading best practices and cutting-edge legal technology.
Representing a broad range of clients including the leading corporates of the region, our clients are at the heart of our practice. In less than a decade, Rahmat Lim & Partners has achieved top-tier rankings by notable legal directories and publications in major practice areas, and regularly receives accolades and recognition from industry watchers.

**www.rahmatlim.com**

RAHMAT LIM & PARTNERS
IN ASSOCIATION WITH ALLEN & GLEDHILL (SINGAPORE)

# Malta


Dr. Emma Grech


Dr. Christina M. Laudi

City Legal

## 1 The Crime of Money Laundering and Criminal Enforcement

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

Anti-money laundering and the combatting of financial terrorism ('AML/CFT') are principally regulated by the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta) ('PMLA') and its subsidiary legislation, the Prevention of Money Laundering and Funding of Terrorism Regulations (Subsidiary Legislation 373.01 of the Laws of Malta) ('PMLFTR'), which have effectively transposed the Fourth AML Directive (Directive (EU) 2015/849 ('4AMLD') and, through recent amendments, the Fifth AML Directive (Directive (EU) 2018/843) ('5AMLD'), into Maltese law.

The investigation and prosecution of money laundering and the funding of terrorism ('ML/FT') are regulated by Article 3 PMLA, whereby every person charged with an offence shall be tried in the Criminal Court or before the Court of Magistrates as a court of criminal judicature in Malta or Gozo and as directed by the Attorney General ('AG'). As elaborated upon in question 1.4 hereunder, the Financial Intelligence Analysis Unit ('FIAU') does not prosecute ML/FT, but aids in the process of prosecution as a result of its supervisory nature.

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

For prosecution to succeed, there must be the conversion or transfer of property with the knowledge or suspicion that such property is derived, whether directly or indirectly, from criminal activity, and this for the purpose of concealing or disguising the origin of the property or assisting those involved in criminal activity. The same applies to the proceeds of said property. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property with the knowledge or suspicion that such property is derived, directly or indirectly, from criminal activity or from an act of participation in criminal activity also constitute ML. Further to this, the acquisition, possession and use of said property and the retention of said property without a reasonable excuse is likewise an offence. Any attempts at these actions as per Article 41 of the Criminal Code (Chapter 9 of the Laws of Malta) ('CC'), or complicity in terms of Article 42 CC, are also defined as ML.

Whereas the underlying criminal activity (predicate offence) from which funds originate is an essential element for prosecution, Article 2(2) PMLA specifically states that a person may still be convicted of ML in the absence of a judicial finding of guilt in respect of the underlying criminal activity. Its existence may be established through circumstantial or other evidence without it being necessary for the prosecution to prove or specifically pinpoint the criminal activity. A person can be accused of ML even though the predicate offence has not been established, as long as it can be proved beyond reasonable doubt that the source of such money or property was derived from criminal activity. The offender may be charged separately for the predicate offence.

As of 31 May 2005, and via Legal Notice 176 of 2005, Malta no longer has a restricted list of predicate offences. All criminal offences are predicate offences. Tipping off is also an offence. As a defence, the accused must prove that he did not know or did not suspect that the disclosure was likely to prejudice the investigation. Tax evasion and all related tax crimes are also deemed to be predicate offences.

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

Article 9 PMLA refers to situations which involve proceeds found outside of Malta, and the powers of investigation by Maltese authorities in connection with offences cognisable by courts outside of Malta. Article 10 PMLA deals with an extraterritorial request to the AG for the temporary seizure of all or any of the moneys or property, movable or immovable, or a person charged or accused in proceedings before extraterritorial courts. Conflicts arise in scenarios where the predicate offence is or is not a crime in that relative jurisdiction.

The FIAU also features in the context of cross-border cases. It cooperates with similar foreign, national and supranational bodies, authorities and/or agencies in coordinating and exchanging information and in imposing administrative penalties and/or implementing other measures.

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

The FIAU is the government agency established under the PMLA responsible for collecting, processing, analysing and disseminating information with the scope of preventing ML/FT and ensuring compliance with the relevant laws and regulations. Upon receiving a report or tracking irregular activity, it must forward said report to the Commissioner of Police.

The investigative process is led by the Economic Crimes Unit within the Malta Police Force, more specifically the Money Laundering Unit. It secures evidence and witnesses both internationally and nationally. It is the police who proceed to prosecute in court in conjunction with the AG's office. The AG directs how a person is to be charged with the relative offence after taking into consideration various factors, including the person's age and the value of the property allegedly laundered.

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

Yes, corporate liability is included. Article 3(2) PMLA states that when an offence is committed by a body or persons, whether corporate or unincorporate, every person who at the time of the commission of the offence had an executive or administrative role shall be guilty of an offence unless he proves that the offence was committed without that person's knowledge and that he exercised all due diligence to prevent the commission of the crime. Article 3(4) PMLA specifically vests legal representation in the alleged offender, and where said legal representation no longer vests in that person, it shall lie with the replacing persons in his/her stead or other referred persons.

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

Article 3(1) PMLA establishes that the maximum punishment is a fine not exceeding €2,500,000 or imprisonment for a period not exceeding 18 years or both. As for legal entities, there are three punishments: that given to the actual individual within the corporate body; the penalty given to the corporate body; and the subsequent forfeiture of proceeds of the corporate body by the Government.

Furthermore, non-compliance with the ML/FT procedures under the PMLFTR is punishable with administrative sanctions reaching a maximum of a €50,000 fine and/or two years' imprisonment.

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

As the PMLA establishes a maximum penalty of 18 years' imprisonment for ML offences, the CC states that crimes liable to imprisonment for a term of not less than 20 years are barred by the lapse of 15 years; whereas the PMLFTR awards two years' imprisonment, and then these crimes are barred by the lapse of five years.

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

Enforcement is at a national level as Malta is an island and has no provinces/states.

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

The PMLA provides for the confiscation of property. In addition to Article 23 CC, i.e. the forfeiture of the *corpus delicti* (evidence of the crime), the court shall order the forfeiture of the proceeds in favour of the Government or of such property the value of which corresponds to the value of such proceeds (any economic advantage), and any property in the possession or under the control of any person found guilty and deemed to be derived from the offence of ML. The definition of 'property' includes movables or immovables, in or outside of Malta.

Article 4 of the Confiscation Orders (Execution in the European Union) Regulations (Subsidiary Legislation 9.15 of the Laws of Malta) states that the AG is competent to receive confiscation orders issued in the issuing State and to transmit to the executing State his own confiscation orders as issued in Malta by a court of criminal jurisdiction. When the AG receives a request by a judicial authority to be enforced in Malta made by a foreign court, an action is brought. Following legal procedures and a hearing, if enforcement of the order is obtained, then the property is confiscated by the Government. The AG may issue the precautionary acts needed. Confiscation can be an additional punishment to a fine and/or imprisonment, or it can occur via an order made by Malta or to Malta and subsequently enforced through a judgment given by the civil courts. The latter can occur without a criminal conviction and has more of a precautionary nature.

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

No convictions against said institutions and individuals exist.

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

Criminal actions are resolved through the courts. There are instances where a lesser sentence of imprisonment is given in return for a larger fine. In addition, the FIAU imposes administrative sanctions which are public. In November 2019 a local bank appealed the administrative penalties it was given in May 2018 by the FIAU via the Court of Appeal, only to have said penalties confirmed in the amount of €57,500.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

The FIAU is responsible for imposing AML/CFT requirements on all 'subject persons' and is regulated under Part II PMLA. It has recently also become responsible for the Central Bank Account Registry, a centralised automated mechanism for Malta (which shall be regulated by the relative subsidiary legislation), and is now enabled to supervise the implementation and enforcement of any future legislative provision on cash restrictions. It has published the sector-specific Implementing Procedures Part I and Part II ('IPI/IPII') which must be adhered to by subject persons. The IPI/IPII comprise an interpretive tool for the PMLA/PMLFTR while simultaneously assisting subject

persons in designing systems for the prevention and detection of ML/FT. Measures to be taken include customer due diligence ('CDD'), mandatory risk procedures and the use of a risk-based approach, diligent recordkeeping and reporting procedures, and the provision of training to employees. For further information, refer to question 3.1.

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

Reference is made to supervisory authorities which are deemed to be agents of the FIAU. The FIAU on request or upon its own motion shall cooperate and exchange information with a supervisory authority when this would assist in AML and CFT. The Malta Financial Services Authority ('MFSA') conducts supervision amongst financial services licence holders and the Malta Gaming Authority does the same amongst licensed gaming operators. The subject person is nonetheless always responsible for providing the information requested.

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

Supervisory bodies are limitedly responsible for compliance and enforcement as they monitor their members passing on information to the FIAU, which then takes enforcement action.

**2.4 Are there requirements only at national level?**

Currently, the requirements are only at a national level, as Malta is an island and has no states/provinces. These comprise, predominantly, the PMLA, the PMLFTR, the National Coordinating Committee on Combating ML/FT Regulations (Subsidiary Legislation 373.02 of the Laws of Malta) as well as the IPI/IPII.

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

Supervisory bodies aid the FIAU with compliance and monitoring in specific areas and professions. The FIAU then enforces, whilst overall retaining its compliance and monitoring obligations. All of the criteria that would lead to investigations are available on the FIAU website (http://www.fiumalta.org/).

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

The FIAU is Malta's designated government FIU agency.

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

Refer to question 1.7 for the applicable statute of limitations.

For details regarding the FIAU, refer to the information contained in the above questions.

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

The FIAU can in these cases act without the need for a court hearing and judgment. Under the PMLFTR, administrative failures are:

- non-compliance with procedures to prevent ML/FT, such as:
  - failing to maintain/apply procedures for CDD, record-keeping and reporting; and
  - failing to establish internal control, risk assessment, risk management, compliance management and communications;
- commission of an offence under the PMLFTR by corporate/unincorporated bodies and other associations of persons;
- false declaration/false representation by an applicant for business;
- failure to carry out CDD (certain exemptions are applicable to electronic money businesses);
- failure to carry out reporting procedures and obligations;
- tipping off; and
- non-compliance with the IP, guidance and directives issued by the FIAU in terms of the PMLA and PMLFTR.

Administrative penalties may not exceed €50,000. There are a number of fines awarded in addition to imprisonment under the PMLA and these do not exceed €11,646.87.

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

The PMLFTR provides for reprimands in writing. It can also give one-time fixed penalties and/or penalties on a daily cumulative basis. The minimum daily penalty levied is of €250.

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

Apart from the PMLA, the PMLFTR provide for criminal sanctions, such as:

- non-compliance with procedures (Regulation 4(5));
- a false declaration/false representation by an applicant for business (Regulation 7(10)); and
- tipping off (Regulation 16(1)).

The first two categories above are subject to a fine not exceeding €50,000, whereas the third category is subject to a fine not exceeding €115,000, with each category being alternatively subject to imprisonment for a term not exceeding two years, or to both the relevant fine and imprisonment. A disqualification order can also be imposed on company officials for a specified period set by the courts, which may be a minimum of one year and a maximum of 15 years.

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

When a sanction is imposed by the FIAU under the PMLFTR, the

subject person is informed of the potential breach detected and the possibility of an administrative sanction. Representations by the person are requested, following which an internal evaluation is made by the Compliance Monitoring Committee. Should fault be found, reasons shall be given. Said sanction must be paid within 14 days. Instead of sanctions, warnings in writing may also be issued as well as in the course of its compliance/monitoring function. If a person feels aggrieved and the sanction exceeds €5,000, an appeal may be lodged both on points of fact and law. The appeal shall lie to the Court of Appeal (Inferior Jurisdiction) and, following recent amendments on the basis of MONEYVAL's recommendations, the appeal shall be held within three months from the date of filing and a final judgment must be given by the Court within six months of the date of the hearing – and such in default of any agreement by both parties that permits further delay, or exceptional circumstances.

In terms of the revised Article 13C, amending the PMLA via Act 1 of 2020, the FIAU is to publish all administrative penalties and other measures it imposes in terms of the PMLFTR as provided for in the said provision and in accordance with policies and procedures established by the Board of Governors of the FIAU. Both administrative penalties as well as administrative measures are subject to publication. However, the quantum of the administrative penalty as well as the circumstances in which other administrative measures are imposed will determine the information to be published. The threshold of publication has increased from that of €10,000 to €50,000. Further policies and procedures regarding publications have also been promulgated.

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

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

As mentioned further above, AML/CFT requirements are applicable to 'subject persons', which are defined in Regulation 2 PMLFTR as 'any legal or natural person carrying out either relevant financial business or relevant activity'.

'Relevant activity' includes, when acting in the exercise of their professional activities: auditors; external accountants; tax advisors; real estate agents; in the context of particular transactions, such as when they assist clients with the opening of bank accounts or the creation of companies, independent legal professionals, including lawyers; fiduciary and company service providers; licensed gaming operators; and, where the transaction in question involves payment in cash of €10,000 or more, persons engaged in the trading of goods. Notably, Legal Notice 26 of 2020 has recently amended Regulation 2 PMLFTR to include, within the relevant activity category, the provision of intermediation services in relation to property letting by real estate agents where the monthly rent amounts to €10,000 or more.

In turn, 'relevant financial business' covers: activities carried out by the credit institutions; payment institutions and electronic money institutions; insurance undertakings and intermediaries; recognised, licensed or notified collective investment schemes and fund administrators; service providers licensed under the Investment Services Act (Chapter 370 of the Laws of Malta); service providers licensed under the Retirement Pensions Act (Chapter 514 of the Laws of Malta); safe custody service providers; regulated markets and the Central Securities Depository; virtual financial assets ('VFA') agents and licence holders within the meaning of the Virtual Financial Assets Act (Chapter 590 of the Laws of Malta) ('VFAA') and issuers of virtual financial assets; and any other associated activity. Any of the above relevant financial business activities carried out by branches established in Malta will also be subject to AML/CFT requirements.

The requirements, as principally deriving from the PMLA/PMLFTR, IPI/IPII, render it incumbent upon subject persons – including financial institutions – to implement robust AML/CFT systems and policies and procedures, including record-keeping, reporting processes and internal controls. Subject persons are compelled to provide information to the relevant authorities on request. In addition, subject persons are required to submit a sector-specific annual Risk Evaluation Questionnaire to the FIAU regarding their set-up, risk assessment, and preventative measures.

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

AML/CFT requirements are to be likewise applied to VFA agents, licence holders under the VFAA and issuers of VFA. Earlier this year, the FIAU published sector-specific IPII applicable to the VFA industry. The said IPII's applicability, however, also extends to persons who may not be licensed as VFA service providers in terms of the VFAA, but who may be handling VFAs in the course of carrying out relevant financial business or activity, such as, for instance, a custodian or a collective investment scheme. The VFA IPII also contains an annex which indicatively outlines various VFA sector 'red flags' and case studies which are intended to assist the relevant subject persons in further understanding what they are required to look out for when formulating their internal AML/CFT policies and procedures.

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

Yes. Regulation 5(5) PMLFTR imposes the requirement on subject persons – including financial institutions – to, in a manner that is appropriate to the size and nature of the business, have effective AML/CFT systems and policies and procedures, as well as internal controls, in place. Subject persons are required to implement compliance management processes, employee screening policies and training programmes, as well as adopt sufficient reporting mechanisms. Where proportionate, an independent audit function should be set up to test these internal controls.

In addition, subject persons must appoint a Money Laundering Reporting Officer ('MLRO') who will assist in the coordination of its AML/CFT framework. The MLRO will be responsible for the oversight of the subject person's AML/CFT compliance.

Businesses are required to detail their compliance programmes in an internal AML/CFT procedures manual.

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

There are no fixed 'thresholds' *vis-à-vis* large transactions. Subject persons faced with sizable transactions are bound to comply with general AML/CFT recordkeeping and reporting requirements as set out, predominantly, in Regulations 13 and 15 PMLFTR. That said, however, Regulation 11(9), as further supplemented by the IPI, particularly Chapter 3 [The Risk-Based Approach] and 4 [Customer Due Diligence] thereof, stipulates that subject persons are to pay special attention to 'complex' and 'unusually large' transactions which 'are conducted in an unusual pattern' and 'have no apparent economic or lawful purpose'. The findings, which should be recorded by the subject person, should not automatically be reported to the FIAU or the relevant supervisory authority, but instead made available on request.

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

No, there are currently no routine-based reporting requirements.

The obligation to report arises in the context of suspicious activity. Such reporting is to be carried out with due regard to the requirement in Regulation 15(3) PMLFTR. This states that, where a subject person knows, suspects or has reasonable grounds to suspect that funds are the proceeds of crime or are related to FT, or that a person may have been, is, or may be connected with ML/FT, that subject person is to report the same to the FIAU via a Suspicious Transaction Report ('STR'). An STR is to be made as soon as is reasonably practicable, but no later than five working days from when the knowledge or suspicion first arose. STRs should be submitted to the FIAU in accordance with the guidance provided on the FIAU website.

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

There are no specific reporting requirements regarding cross-border transactions. Subject persons are, however, required to inform the FIAU of any business relationships or transactions with persons from 'non-reputable jurisdictions' – as defined in Regulation 2 PMLFTR – if there is an international call for countermeasures (i.e. FATF Category 1/Commission Delegated Regulation identifying high-risk third countries with strategic deficiencies Category III). In this scenario, and following the new Regulation 11(11) PMLFTR as introduced by Legal Notice 26 of 2020, the FIAU or the relevant supervisory authority must adopt any one or more of the listed measures which include, *inter alia*, the prohibition of pursuing the relevant activity or relevant financial activity in Malta or the non-reputable jurisdiction in question.

In the absence of an international call for countermeasures, and when dealing with non-reputable jurisdictions, subject persons shall adopt stricter due diligence measures as outlined in Regulation 11(10) PMLFTR.

In addition, reference must be made to the obligation to submit STRs as outlined in question 3.5 above.

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

Subject persons – including financial institutions – are to establish due diligence procedures for identifying and verifying the identity of a prospective customer. A customer may be a legal or natural person who: (i) seeks to form, or has formed, a business relationship with a subject person; or (ii) seeks to carry out an occasional transaction with a subject person.

CDD measures shall, however, only be applied in the context of occasional transactions when these involve: (i) a transaction of €15,000 or more; (ii) a money transfer or remittance within the meaning of the EU Funds Transfer Regulation (Regulation (EU) 2015/847) (the 'Funds Transfer Regulation') amounting to €1,000 or more; and (iii) a transaction of €2,000 or more in the context of licensed gaming operators. The incorporation of companies and/or the provision of tax advice by subject persons shall also be considered to constitute 'occasional transactions', thereby necessitating CDD.

In the context of business relationships, and following the verification of a prospective customer's details, which verification is carried out by the subject person by – as the case may be – viewing official documentation issued by independent sources, such as a government authority, the subject person will need to obtain details on the purpose and intended nature of said relationship. The information the subject person may need to collect in these circumstances includes: data of the customer's business or employment; the source and origin of funds the customer will be using in the business relationship; and the expected level and nature of the activity to be undertaken through the relationship. This information must be kept up to date, thereby enabling a business to amend its customer risk assessment if circumstances change, and, if necessary, carry out further CDD.

In higher-risk situations, subject persons must apply enhanced due diligence, namely: (i) where the customer has not been physically present for identification purposes; (ii) when transacting with politically exposed persons, or 'PEPs', such as Heads of State and Members of Parliament; (iii) in a cross-border correspondent banking relationship scenario; (iv) where the business relationship or a transaction is connected to be a 'high-risk' jurisdiction (as acknowledged by the EU); and, generally (v) any situation where there may be a greater risk of ML/FT. Enhanced due diligence may necessitate: (i) obtaining additional information to establish the customer's identity; (ii) applying supplementary measures to check the documentation supplied; and (iii) taking adequate steps to establish the source of wealth and funds involved.

Chapters 3 and 4 IPI provide further in-depth guidelines mirroring the above customer due diligence and ongoing monitoring obligations incumbent upon subject persons.

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

In terms of Regulation 11(4) PMLFTR, subject persons carrying out relevant financial business are prohibited from entering or continuing correspondent relationships with shell institutions. Moreover, they are required to take appropriate measures to ensure that they do not enter into or continue correspondent relationships with respondent institutions which are known to permit their accounts to be used by shell institutions.

Regulation 2 PMLFTR defines a 'shell institution' as an institution carrying out activities equivalent to relevant financial business, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is not affiliated with a regulated financial group.

**3.9 What is the criteria for reporting suspicious activity?**

Refer to question 3.5.

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

Maltese companies, partnerships, foundations, trusts and associations must identify and maintain a register of their ultimate beneficial owner(s) ('UBO/s') as well as provide this information to, respectively: (i) the Registrar of Companies, in the case of companies and partnerships; (ii) the MFSA, in the case of trusts; and (iii) the Registrar for Legal Persons in the case of associations and foundations, that each maintain UBO registers. This information will be made available to the FIAU.

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

Payment service providers ('PSPs') are subject to the PMLFTR, which, in turn, mandate that any such entities adhere with the provisions of the Funds Transfer Regulation. Full information of the payer and payee – namely name, address and payment account number – must accompany all wire transfers, barring some exceptions. For example, if the PSPs of the originator and the beneficiary are both EU-based, the transfer need only be accompanied by the account number.

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

No. Ownership of shares is evidenced by their entry into a company's share register and by the issue of share certificates.

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

Generally, the PMLA/PMLFTR apply in a like manner to all the persons listed in question 3.1, which include certain non-financial institution businesses.

There are some exceptions, such as the privilege applicable to various professionals, including lawyers, which in turn are exempt from the duty to report suspicious transactions to the FIAU in accordance with Regulation 15(9) PMLFTR in certain instances. Some additional requirements are imposed on PSPs, which must comply with the Funds Transfer Regulation (refer to question 3.11 above). In addition, gaming operators must comply with the IPII for the Remote Gaming Sector (which are currently being revised, but which remain applicable until the date of their revision) and/or Land-Based Casinos, as may be the case, while the sector-specific IPII applicable to the VFA industry regulate the various stakeholders participating, in some manner, in services governed by the VFAA (refer to question 3.2 above). It is also noteworthy that the IPII for the Banking Sector have recently been repealed, and are expected to be replaced with a new set of banking-specific IPII which will find their applicability to credit institutions.

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

Aside from the business activities listed in question 3.1 above, there are no AML requirements applicable to other specific business sectors.

In terms of the IPI, customer risk and geographical risk are two of the factors that must be considered as part of a subject person's ML/FT risk assessment.

## 4 General

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

On 17 July 2019, the FIAU published a revised version of the IPI reflecting the legislative amendments which took place between December 2017 and January 2018 to the PMLA/PMLFTR following the transposition of 4AMLD.

As stated in question 3.2, the VFA IPII were issued earlier this year. The issuance of public consultations regarding sector-specific IPII for corporate service providers, the Banking Sector, the Insurance Sector, trustees and fiduciaries, as well as the revised Remote Gaming Sector IPII, is expected in due course.

On 14 October 2019, the FIAU published a consultation document laying down the proposed amendments to the PMLFTR with the aim of transposing the 5AMLD. The amendments were adopted in February 2020 with slight variations from the consultation document. With these latest amendments, the 5AMLD has been definitively transposed into local legislation.

In addition, the MFSA launched its Vision 2021 in January 2019, which comprises a comprehensive strategy designed to clamp down on ML/FT in the financial services sector.

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

Following MONEYVAL's Fifth Round of Evaluation on-site visit in November 2018, the Mutual Evaluation Report adopted during MONEYVAL's 58th Plenary Meeting in July 2019 observed that since its last review, Malta has indeed taken steps to improve its AML/CFT framework, but that the jurisdiction should strengthen its efforts to engage in more effective implementation – and enforcement – of the applicable rules. The Report found Malta to be 'Compliant' with 10 FATF Recommendations, 'Largely Compliant' with 21, and 'Partially Compliant' with nine. MONEYVAL has invited Malta to report back in December 2021.

Pursuant to MONEYVAL's Report, the Venice Commission's December 2018 opinion on Malta's constitutional arrangements, separation of powers and the independence of the judiciary and law enforcement, as well as the transposition of the 5AMLD, the PMLA and the PMLFTR were amended earlier this year to enhance the FIAU's functions and powers. With the objective of strengthening the FIAU's independence and effectiveness, its Director shall now be appointed after a public call for applications, whereas the Attorney General has been removed from the its Board of Governors. Enhanced measures have also been introduced addressing business relationships and transactions involving non-reputable jurisdictions.

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

The latest evaluation was carried out by MONEYVAL following the Fifth Round of Evaluation on-site visit to Malta in November 2018. For further information regarding the recommendations published in MONEYVAL's Evaluation Report, please access the Council of Europe website (https://www.coe.int/en/web/moneyval/jurisdictions/malta).

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

Yes, all sources are available in English.

Reference is made to the website of the Ministry for Justice, Culture and Local Government (https://legislation.mt/), where local legislation and regulations, including AML/CFT rules and regulations, may be accessed. In addition, the FIAU website enlists further information such as the IPI/IPII, additional guidance, FATF statements and MONEYVAL evaluations. The MFSA website (https://www.mfsa.com.mt/) also comprises substantial information on AML/CFT, including circulars and public consultations affecting the financial sector.

**Dr. Emma Grech** is a practising lawyer, having graduated as Doctor of Laws from the University of Malta in 2015 after submitting her thesis, entitled 'Regulating the Future? The Legal Implications of Social Games'. Thereafter, she embarked on an LL.M. in Banking and Finance Law at the University of London. Emma joined City Legal in January 2018 and was made Partner in June 2019. Her main areas of practice at the firm are corporate finance and re-structuring, gambling and betting, anti-money laundering and data protection regulation. She advises on the legal and regulatory aspects of each of these areas, as well as the implications thereof on clients' business models. She frequently assists in a range of local and cross-border transactions involving her areas of specialisation. Emma also occupies the role of company secretary in various companies, including listed entities.

**City Legal**
Britannia House, Suite 8
Old Bakery Street
Valletta
Malta

Tel: +356 2744 1120, +356 2744 1121
Email: emma.grech@thecitylegal.com
URL: www.thecitylegal.com

**Dr. Christina M. Laudi** is a Partner at City Legal, and has been practising law with the firm since 2014 after having obtained her Doctor of Laws from the University of Malta in 2013. Her doctoral thesis was entitled 'Criminal Liability in Animal Welfare: A Comparative and Critical Analysis'. Following this, Christina read for an LL.M. in Family Law with the University of London, where she graduated in 2017. Christina's main areas of practice are family law, civil law, residence and immigration law as well as anti-money laundering regulation. Christina provides advice on various family law matters such as separation, divorce, care and custody issues as well as various civil law issues ranging from property law to damages and personal injury. Christina has also taken an active interest in the subject of financial crime and advises clients on matters of anti-money laundering regulation.

**City Legal**
Britannia House, Suite 8
Old Bakery Street
Valletta
Malta

Tel: +356 2744 1120, +356 2744 1121
Email: christina.laudi@thecitylegal.com
URL: www.thecitylegal.com

City Legal is a boutique law firm with offices in Valletta that has, throughout recent years, adopted an innovative approach focused on offering customised legal services in a manner which encourages its lawyers to combine specialist sector knowledge with a personalised service, resulting in the delivery of commercially focused and high-quality legal advice.

Committed to this approach, the firm's lawyers consider themselves partners in their clients' businesses, taking pride in their clients' achievements, and constantly looking to establish strong, trusted, and lasting relationships with them.

We consider foreign-based law firms, corporate service providers, and other professionals including accountants, licensed trustees, tax advisers, and IT specialists to be our partners on the international front. Having ensured a regular overseas presence, the firm has established a robust international client-base which complements its local operations.

**www.thecitylegal.com**

City | Legal

# Mexico


Humberto Pérez-Rocha Ituarte


Claudio Kurc Citrin

Galicia Abogados, S.C.



## 1 The Crime of Money Laundering and Criminal Enforcement

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

The Attorney General Office (*Fiscalía General de la República*) is in charge of prosecuting money-laundering activities at the national level, with the support of the Ministry of Finance and Public Credit through the Financial Intelligence Unit ("FIU").

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

Article 400 *Bis* of the Mexican Federal Criminal Code describes the following crimes related to money laundering:

- Acquiring, selling, safeguarding, possessing, transforming, depositing, investing, withdrawing, transferring and transporting resources, assets or rights of any kind within Mexico or from Mexico to other countries and *vice versa*, with prior knowledge that such resources, rights or assets are related to illegal activities.
- Concealing or covering up (or attempting to cover up) the nature, source, location, destination or ownership of resources, rights and assets with prior knowledge that such resources, rights or assets are related to illegal activities.

Tax evasion is not necessarily a predicate offence for money laundering; however, in case it is framed as one of the activities mentioned above, it may be considered as a money-laundering activity.

### 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 money-laundering crimes when such crimes are initiated or executed in foreign territory and have effects in Mexico.

There is also extraterritorial jurisdiction when all of the following conditions are met:

(i) based on an international treaty, Mexico may extradite or judge such criminal offence;
(ii) the accused person is located in Mexico;
(iii) no final ruling has been issued in the country in which the crime was committed;
(iv) money laundering (or any other crime) is considered a crime in the country in which it was carried out; and
(v) the accused person has not been extradited.

Money laundering of the proceeds of foreign crimes may be punishable insofar the requirements set forth in questions 1.2 and 1.3 are met.

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

The government authority responsible for investigating money laundering crimes is the FIU, and the authority responsible for prosecuting such crime is the Attorney General Office.

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

Under the National Code for Criminal Procedures (*Código Nacional de Procedimientos Penales*), legal entities are liable for criminal offences: (i) if such crime is carried out on its behalf, by its instructions, in its benefit or through means provided by the company; and (ii) if the company does not comply with due control mechanisms.

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

The maximum penalties applicable to money-laundering criminal offences are normally 15 years; however, such amount may be increased for a total of 30 years of prison in certain cases. The maximum penalty amount is approximately US$46,459.

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

The statute of limitations for money-laundering crimes shall be the arithmetic average of the established penalties. Therefore, the ordinary statute of limitations is nine years; however, such statutes of limitations may be increased to 20 years for particularly serious scenarios. Furthermore, please note that statutes of limitations may be doubled in case the accused person is located in another foreign country and such person has not been prosecuted for such reason.

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

Enforcement of money-laundering crimes may occur at national or local levels. Most local (state level) regulation regarding money-laundering crimes is substantially similar to the regulation applicable 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?**

Under the National Law for Extinction of Ownership, the Fiscal Office (*Ministerio Público*), the Attorney General Office and the Institute for the Administration of Goods and Assets (*Instituto para la Administración de Bienes y Activos*) are the authorities related to confiscations. Funds or property may be confiscated when they are used by, are related to, or are the result of certain illegal activities, including money laundering. Please note that, under certain cases, the funds and property subject to a confiscation procedure may be sold or disposed of by the government prior to the issuance of a final ruling by the authority.

Furthermore, there can be confiscation of funds and property even if there has been no criminal conviction, as long as there is enough evidence to suggest that those funds and property have been used by, are related to, or are the result of certain illegal activities.

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

There have been no money-laundering convictions of banks, financial institutions or their corresponding directors and employees. However, HSBC Mexico was convicted for money-laundering offences in 2012, and received a severe monetary fine from the National Banking and Securities Commission.

**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?**

As a general rule, criminal actions are always resolved through a judicial process. However, certain criminal actions, including those related to financial crimes committed without violence, may be resolved through negotiations between the defendant and the plaintiff. Such negotiations must comply with certain formalities and eventually must be approved by the Fiscal Office or the corresponding judge.

On November 2019, the Mexican Congress approved an amendment to the Transparency Act (*Ley General para la Transparencia y Acceso a la Información Pública*) in order to make all criminal rulings public. However, criminal actions resolved or settled through alternative mechanisms (i.e. other than judicial process) do not appear to be contemplated as part of such amendment.

## 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 Mexican law, AML regulation may be broadly divided in two: (i) financial institutions; and (ii) non-financial institution businesses that carry out relevant activities. AML money requirements applicable to financial institutions are more burdensome than those applicable to other type of businesses.

The authorities responsible for imposing AML requirements on financial entities will vary depending on the nature of the financial activity and are the following:

(i) Ministry of Finance and Public Credit (*Secretaría de Hacienda y Crédito Público* or "SHCP");
(ii) National Securities and Banking Commission (*Comisión Nacional Bancaria y de Valores* or "CNBV");
(iii) National Insurance and Bond Commission (*Comisión Nacional de Seguros y Fianzas* or "CNSF");
(iv) National Retirement and Savings System Commission (*Comisión Nacional de Sistema de Ahorro para el Retiro* or "CONSAR");
(v) FIU (*Unidad de Inteligencia Financiera*); and
(vi) Tax Administration Service (*Servicio de Administración Tributaria* or "SAT"), for non-financial businesses.

As mentioned above, AML requirements and the corresponding degree of compliance may differ depending on the type of entity or business; however, generally speaking the following requirements are always applicable:

(i) For non-financial institution businesses, the Federal AML Act (*Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita*) sets forth the following obligations:
- know-your-customer ("KYC") obligations;
- client risk assessments;
- general AML reports;
- AML policies; and
- information storage.

(ii) For financial institutions, each of their corresponding applicable regulations set forth the following obligations:
- KYC obligations;
- client risk assessments;
- several types of suspicious activity reports;
- AML policies;
- appointment of a Compliance Officer;
- appointment of an AML Committee;
- automated systems; and
- information storage.

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

No, there are no such requirements.

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

No, they are not responsible.

**2.4 Are there requirements only at national level?**

Yes. All AML requirements are applicable at a national level. AML local regulation is not applicable to financial entities.

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

Regarding financial institutions, the competent authorities for examination for compliance and enforcement of AML requirements are: (i) the FIU; (ii) the Ministry of Finance and Public Credit; and (iii) depending on the type of financial entity – (a) the National Banking and Securities Commission, (b) the National Insurance and Bond Commission, or (c) the National Retirement and Savings System Commission.

Regarding non-financial businesses, the FIU, the Ministry of Finance and Public Credit and the Tax Administration Service are the competent supervising authorities.

Although no specific criteria for examination are publicly available, generally speaking, all examinations will be carried out based on obligations set forth in the applicable AML regulation. Furthermore, all entities and individuals subject to AML obligations may request the authority to issue an opinion regarding specific criteria for examination. Financial entities should request such criteria from their corresponding regulator, while non-financial businesses should request an opinion from the SAT.

**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, Mexico has a FIU which is part of the Ministry of Finance and is, among other things, responsible for analysing the information reported by financial institutions and other non-financial business, as well as participating in the drafting of applicable AML regulation. The FATF has classified the Mexican FIU as mostly compliant.

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

The statute of limitations to bring enforcement actions regarding AML matters is 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?**

Maximum penalties for failure to comply with AML requirements will depend on the type of corporation that fails to comply with such obligations:

(i) Regarding non-financial institution businesses, the maximum penalties are approximately US$428,304 or 10% of the monetary value of the operation, whichever is greater. Furthermore, the following actions are subject to penalty provisions: (i) failure to comply with requirements requested by the regulator; (ii) failure to comply with obligations related to KYC and information storage; (iii) not issuing AML reports on time; (iv) issuing incomplete AML reports; (v) not issuing AML reports; and (vi) accepting cash as consideration for certain transactions (e.g. real state acquisition) or accepting cash in excess of the limits set forth by the Federal AML Act.

(ii) Regarding financial institutions, penalties will depend on the type of financial institution; however, the maximum penalties are approximately US$627,754 for each operation or 100% of the amount corresponding to the operations that were not duly reported.

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

In addition to monetary penalties, non-financial institution businesses that carry out the following activities may have their licences revoked in case of repeated breach of AML obligations: (i) gambling and lottery activities; (ii) international trade customs activities; and (iii) notary publics. Furthermore, under certain scenarios, failure to comply with AML regulation may also result in criminal sanctions.

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

Criminal sanctions related to AML obligations are only applicable when: (i) an individual intentionally modifies or alters any information or documentation related to AML reports; and (ii) when an individual discloses information related to AML reports without prior authorisation by the regulator.

**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 assessment of sanctions must result from a previous administrative proceeding whereby the competent authority provides the alleged offender with 15 business days to file legal arguments and evidence to prove that no infringement to the law has taken place. Sanction proceedings may (or may not) derive from previous verification proceedings carried out on the company's premises.

In case a monetary sanction is imposed, a request for collection is sent to and carried out by the Tax Administration Service ("SAT"). Absent a judicial injunction preventing the collection of the sanction, the SAT formally notifies the debtor requesting immediate payment. If no payment is made at the time of the visit, the SAT may seize assets based on the amounts due.

Decisions imposing sanctions may be appealed either by an administrative appeal before the Ministry of Finance and Public Credit or by an annulment claim before the Federal Tribunal on Administrative Matters, which may also issue an injunction preventing collection measures.

Resolutions of penalty actions by competent authorities shall only be public in case a specific law provides that some

general information is made available to the public. Examples of public penalties include those issued by the CNBV (*e.g.* banks, brokerage houses) and the CNSF (*e.g.* insurance companies, bond companies).

Financial institutions usually challenge 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 following financial institutions are subject to AML requirements:

- banks;
- multi-purpose financial institutions ("SOFOMs");
- securities brokers;
- general bonded warehouses;
- money exchange centres;
- money exchange brokers;
- money transmitters;
- investment funds;
- investment advisors;
- savings and retirement managers and funds;
- credit unions;
- popular financial entities (*sociedad financiera popular*);
- saving and credit cooperative companies (*sociedad cooperativa de ahorro y préstamo*);
- bonding companies;
- insurance companies;
- crowdfunding institutions;
- electronic money institutions; and
- regulatory sandbox players.

The following professional activities carried out by non-financial businesses are subject to AML requirements. Please note that certain activities are only regulated once a certain threshold has been exceeded:

- gambling and lottery activities;
- issuance, marketing and sale of credit cards, debit cards, prepaid cards, and any other type of money storage mechanisms not issued or sold by financial institutions;
- issuance and sale of traveller cheques not issued by financial institutions;
- loan activities;
- real estate and construction activities;
- sale of precious metals, jewellery and watches;
- auction or sale of art;
- sale of vehicles, either used or new;
- vehicle armour plating services;
- money transport services;
- resource management services and rendering professional services on behalf and in the name of clients;
- services rendered by attesting officials;
- donations by authorised donors;
- international trade activities;
- real estate leasing activities; and
- cryptocurrency activities.

For information regarding the general obligations applicable to individuals and entities subject to AML regulation, please refer to question 2.1 above.

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

In Mexico, there are two separate regulatory frameworks under which AML requirements are applied to the cryptocurrency industry.

On one hand, the Federal AML Act sets forth that the following activities carried out by non-financial businesses are subject to the general AML compliance obligations:

(i) cryptocurrency exchange services through digital interfaces;
(ii) cryptocurrency management and/or operation services;
(iii) services that facilitate the purchase and/or sale of cryptocurrencies;
(iv) cryptocurrency custody and storage services; and
(v) cryptocurrency transmission services.

On the other hand, the Mexican Fintech Act (*Ley para Regular las Instituciones de Tecnología Financiera*) allows electronic money institutions, crowdfunding institutions and banks to offer certain cryptocurrency-related services to the public, insofar as they obtain a specific authorisation from the Mexican Central Bank, which shall be granted on a case-by-case basis and is subject to certain non-minor restrictions (i.e. only internal or closed loop transactions are permissible).

Such financial institutions are subject to their own exhaustive anti-money laundering frameworks, as described in question 2.1 above.

It is important to note that, as a FATF signatory, Mexico is working towards implementing legal mechanisms to enforce Recommendation 16 within the jurisdiction, thus obliging the abovementioned entities (i.e. virtual asset service providers) to comply with the so-called "travel rule" in cases where customer transactions exceed provided thresholds.

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

All persons subject to AML obligations must develop and implement compliance programmes: (i) regarding non-regulated businesses, such programmes must include KYC policies and information-sharing policies; and (ii) regarding financial institutions, such programmes must include KYC policies, a risk assessment methodology, and mechanisms to be employed in order to comply with the obligations set forth in question 2.1.

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

All AML-related information must be kept for a term of at least 10 years. Regarding large currency transactions, all transactions that exceed US$7,500 must be reported during the first 10 business days of January, April, July and October through electronic means.

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

- Unusual Activity Report: (i) Any client activity which does not match the client's background and regular behaviour

regarding the destination or origin of the resources, or the amounts, frequency or nature of the corresponding operation whenever no reasonable justification is apparent; or (ii) any operation which the financial entity has reason to believe is intended for money laundering or terrorist activities.

- Suspicious Internal Activity Report: (i) The conduct, activity or behaviour of any of the partners, directors, officers, legal representatives or employees, as well as those who exercise control over the financial entity, whenever such actions may breach regulatory obligations under the AML Regulation; or (ii) any operation which the financial entity has reason to believe is intended for money laundering or terrorist activities.
- 24-Hour Report: Financial entities shall issue a report within 24 hours under the following scenarios: (i) when the financial entity believes that the client or operation may be related to money laundering or terrorist activities; (ii) if continuing the KYC process may warn the client that the financial entity believes that such client is related to money laundering or terrorist activities; and (iii) when the financial entity identifies risks as set forth in its AML policy.

All the reports mentioned above must be filed through the regulator's AML electronic platform.

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

Certain financial institutions shall file a report in connection with each international transfer of funds that, individually, clients have received or sent during said month, for an amount equal to or greater than US$1,000 or the equivalent in the foreign currency used. The financial institutions that are subject to this requirement are: (i) banks; (ii) exchange houses; (iii) saving and credit cooperative companies; (iv) money transmitters; (v) brokerage houses; (vi) popular financial entities; (vii) crowdfunding institutions; and (viii) electronic money institutions.

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

Financial institutions are required to identify all costumers, either through face-to-face mechanisms or through digital means. For individuals, basic identification information is required, while for legal entities, information regarding such entities' legal existence and authorised signatories is required. In all cases, information regarding the ultimate beneficial owner, if any, is required.

Furthermore, customers that are classified as high-risk and politically exposed persons require enhanced due diligence requirements. Applicable law does not include guidelines in connection with such enhanced due diligence requirements.

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

No, as long as such foreign shell banks and/or the countries in which they are licensed are not part of a blocked person list.

**3.9 What is the criteria for reporting suspicious activity?**

Please refer to questions 3.4, 3.5 and 3.6.

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

No. The Mexican government does not assist financial institutions with any type of AML information.

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

Yes. Financial entities must include information about the originators and beneficiaries for a funds transfer, including name, address and account number. Such information must also be included in payment instructions to other financial institutions.

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

No. Bearer shares are not permitted under Mexican law.

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

AML requirements are applicable to non-financial institution businesses who carry out certain relevant activities. However, AML requirements applicable to such businesses are substantially less burdensome than those applicable to financial institutions. Please refer to question 3.1 for more information regarding the types of relevant activities.

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

Rendering international trade services as a customs agent of the following merchandise is considered a relevant activity under the Mexican AML regulation:

- vehicles;
- betting and lottery machines;
- equipment and materials used for payment cards;
- jewellery, precious metals and watches with a value that exceeds the threshold set forth by the AML regulation;
- artwork, with a value that exceeds the threshold set forth by the AML regulation; and
- materials related to armour-plating services.

Please note that the Mexican government issues blacklists based on those provided by certain international organisations. Therefore, additional AML requirements may be applicable regarding operations carried out with individuals or companies from certain foreign jurisdictions.

## 4 General

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

There are no additional AML measures proposed so far.

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

According to the FATF's 2018 evaluation, money-laundering services are not being actively investigated and prosecuted by the Attorney General Office; rather, such investigations have been made in a reactive manner. Among the main impediments for complying is the level of corruption present in all levels of the government as well as a lack of equipment and preparation of the authorities in order to efficiently apply AML mechanisms.

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

Mexico has been subject to evaluations carried out by the FATF. According to the FATF's 2018 review, Mexico has a mature AML/CFT regulatory regime and has reported significant progress since the previous evaluation (2008). Notwithstanding the above, such evaluation determined that Mexico required further actions in order to be fully effective. In particular, non-financial institution businesses have not grasped the risks associated with 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?**

All relevant AML laws, regulations and administrative decrees are publicly available on the internet. However, such documents are not publicly available in English:

AML general regulation applicable to financial entities may be found at: https://www.gob.mx/shcp/documentos/uif-marco-juridico-disposiciones-de-caracter-general.

AML regulation applicable to non-financial institution businesses may be found at: https://sppld.sat.gob.mx/pld/interiores/marco.html.

The Mexican Criminal Federal Code may be found at: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_240120.pdf.

## Acknowledgments

The authors would like to thank Arturo Portilla and Iván Valdespino, associates at Galicia Abogados, for their assistance in the preparation of this chapter.

**Humberto Pérez-Rocha Ituarte** has been a partner of Galicia Abogados, S.C. since 2002. He is an attorney specialised in national and international business transactions and his practice areas include corporate finance, mergers and acquisitions, capital markets and insurance. Additionally, he advises different credit and insurance institutions in their daily operations and regulatory matters, including anti-money laundering.

He has represented the principal participants of the private sector, including insurance companies and financial institutions, telecommunications, textile, agriculture and petrochemical companies in their financing operations, restructuring, strategic alliances and mergers and acquisitions.

Humberto serves as member of the Board of Directors of different corporations, including insurance companies and pension fund managers. Previously, he worked as a foreign associate at Gibson, Dunn & Crutcher LLP. He has a Bachelor's degree in Law from Universidad Iberoamericana.

Humberto has been recognised by several publications, including *IFLR1000*, as an expert lawyer in corporate law, mergers and acquisitions and banking and finance.

**Galicia Abogados, S.C.**
Blvd. Manuel Ávila Camacho #24
7º Piso, Col. Lomas de Chapultepec, 11000
Mexico City
Mexico

Tel: +52 55 5540 9214
Email: hperezrocha@galicia.com.mx
URL: www.galicia.com.mx

**Claudio Kurc Citrin** joined Galicia Abogados in 2017, and is an associate in the Banking and Finance practice area. His work is focused on banking and finance, providing advice to several financial entities regarding M&A, loans and regulatory operations, including anti-money laundering compliance, among others. Further, he has specialised in providing legal advice to several financial entities and companies in connection with fintech regulation.

He has also participated in several audits regarding legal and regulatory risks for financial entities. Claudio has also worked with several financial entities in temporal secondments, carrying out activities as an internal legal advisor.

Prior to joining Galicia Abogados, he worked at the Banking, Securities and Savings Unit of the Ministry of Finance. He studied law at Instituto Tecnológico Autónomo de México.

**Galicia Abogados, S.C.**
Blvd. Manuel Ávila Camacho #24
7º Piso, Col. Lomas de Chapultepec, 11000
Mexico City
Mexico

Tel: +52 55 5540 9243
Email: ckurc@galicia.com.mx
URL: www.galicia.com.mx

Galicia Abogados, S.C. is a leading law firm in Mexico with more than 25 years of experience, helping clients take better business decisions by providing specialised knowledge and with its ability to understand clients' business needs and strategies. Galicia Abogados is a leader in five strategic sectors provided through a multidisciplinary approach from our specialised practices: Finance; Energy & Infrastructure; Private Equity; Real Estate; and Regulated Industries. The firm's unique way of thinking provides solid, innovative and constructive solutions to the challenges faced by clients in light of ever more complex and demanding operations. Galicia Abogados strikes a balanced approach covering and protecting the needs and positions of clients, while making sure the transaction reaches successful closing.

Galicia Abogados has a close relationship with the most important law firms in North and Latin America, Europe and Asia. Most of its attorneys hold graduate degrees and have worked in leading firms in the United States and Europe.

**www.galicia.com.mx**

Galicia

# Myanmar


Minn Naing Oo

Dr. Ei Ei Khin

Allen & Gledhill (Myanmar) Co., Ltd.


## 1 The Crime of Money Laundering and Criminal Enforcement

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

The legal authority to prosecute money laundering offences under the Anti Money Laundering Law 2014 ("**AMLL**") rests with the Financial Intelligence Unit ("**FIU**"), a unit formed by the Central Board of Anti Money Laundering ("**Central Board**") pursuant to the AMLL to investigate and prosecute offences under the AMLL.

Section 68 of the AMLL prescribes that the prior sanction of the Central Board or organisation authorised by the Central Board shall be obtained to prosecute any offences under the AMLL.

As a matter of practice, the police will also need to be involved in any investigation under the AMLL.

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

The government must prove that the act committed falls within the meaning of "Money Laundering" and "Money Laundering" under Section 3(n) of the AMLL, which is defined as the commission of any of the following:

a) converting or transferring money or property, knowing or having reason to know that the money and property are obtained by illegal means, for the purpose of changing or concealing the origin, or whether before or after the commission thereof, for the purpose of assisting a person involved in the commission of an offence to evade the legal action under the AMLL;
b) changing the original nature, source, location and characteristics, or concealing or disguising the ownership or rights of money or property, knowing or having reason to know that the money and property are obtained by illegal means;
c) acquiring, possessing or using money or property, knowing or having reason to know at the time of receipt that money and property are obtained by illegal means; or
d) committing, attempting to commit, or conspiring with intention to commit, or by commission or omission, assisting, supporting, providing, managing, advising, being any member, and by any other means involving any offence mentioned in clause (a) to clause (c).

Section 5 of the AMLL defines the money-laundering predicate offences as being the following:

a) offences committed by organised crimes;
b) offences relating to sexual exploitation including sexual exploitation of children;
c) offences relating to infringement of intellectual property rights;
d) offences relating to environmental crime;
e) offences relating to the evasion of tax and other tax crimes;
f) offences relating to piracy;
g) offences relating to terrorism;
h) offences relating to insider trading wherein the person who is the first to know the information seeks to obtain illicit profits by using the said information himself, or through providing it to another person, or through market manipulation;
i) committing of any offence punishment with imprisonment for a term of a minimum of one year and above under any existing law of Myanmar;
j) offences prescribed by the Union Government that are applied to the AMLL by notification from time to time; and
k) offences relating to cooperation, abetting, supporting, providing, managing, advising and part of a group committing or attempting to commit or conspiring to commit by action or omission of any offence contained in sub-sections (a) to (j) and by any other means.

Yes, tax evasion is a predicate offence for money laundering.

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

Section 2 of the AMLL provides that the AMLL only applies to offences committed within the territories of the Union of Myanmar, or on board a vessel, an aircraft or any motor vehicle registered under an existing law of Myanmar, or a Myanmar citizen or any person residing permanently in the Union of Myanmar who commits the said offence beyond the limits of the country.

There is extraterritorial jurisdiction only for Myanmar citizens or any person residing permanently in the Union of Myanmar or for an act committed on board a vessel, an aircraft or any motor vehicle registered under an existing law of Myanmar.

Money laundering of the proceeds of foreign crimes is punishable only if it falls within the limits of Section 2 of the AMLL.

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

The relevant government authorities are the FIU, Scrutiny Body, Investigation Body and various law enforcement agencies in Myanmar (as set out below).

Chapter V of the AMLL provides that the FIU is the government authority responsible for investigating and prosecuting money-laundering criminal offences.

The FIU shall, after receiving and scrutinising the reports and information under the AMLL, form and assign the Scrutiny Body, the function of which is to scrutinise money laundering, financing of terrorism, money and properties obtained by illegal means and the possessions of terrorists pursuant to Section 14 of the AMLL. Further, an Investigation Body may also be formed by the Central Board to investigate the findings made in the report issued by the Scrutiny Body.

Further, law enforcement agencies in Myanmar which are responsible for detecting, investigating and scrutinising offences in Myanmar will also be responsible for the examination of compliance with and enforcement of anti-money laundering requirements. Such law enforcement agencies include the Myanmar Police force, the Bureau of Special Investigation, Department of Customs and the Department of Immigration and National Registration.

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

Chapter XI of the AMLL on "*Offences and Penalties*" provides that there is both corporate criminal liability and liability for natural persons.

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

The maximum penalty is imprisonment for a term which may extend to 10 years or in the case of a legal entity, a fine of K500 million.

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

There is no period of limitation for criminal offences in Myanmar.

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

Enforcement is only at national level and there are no parallel state or provincial criminal offences for money laundering.

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

No, there is no specific confiscation authority in Myanmar for an offence under the AMLL. A court order for confiscation of property is required for an offence under the AMLL. Under the AMLL, property subject to confiscation would include criminal proceeds and instruments of crime.

If there is no criminal conviction, confiscation is only possible on an administrative basis by: (i) the Customs Department, for money, bearer negotiable instruments, or precious stones or metals, the value of which equals or exceeds an amount determined by the Central Board, in a person's possession or baggage; or arranges for the transportation of such goods via mail or any type of vehicles into or out of Myanmar, which were not declared officially to the Customers Department by the person entering or leaving the territory of Myanmar; and (ii) the Internal Revenue Department for property of corresponding value in the form of a pecuniary penalty order in tax evasion cases.

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

No, we are not currently aware of any banks or other regulated financial institutions or other directors, officers or employees being convicted of money laundering.

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

Criminal actions under the AMLL are resolved through the judicial process. Records of the fact of the judgments rendered by the court are public documents which can be procured from the courts. However, the terms of any settlements made are not publicly available.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

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

The legal or administrative authorities are the Central Board and the Central Bank of Myanmar.

**(i) Central Board**

Pursuant to Section 7 of the AMLL, the Central Board is the authority in charge of laying down policies of anti-money laundering and terrorism financing in Myanmar. In this regard, the Central Board shall form the FIU, which is the government authority responsible for investigating and prosecuting money-laundering criminal offences. The FIU shall, after receiving and scrutinising the reports and information it receives under the AMLL, form and assign the Scrutiny Body, the function of which is to scrutinise money laundering, financing of terrorism, money and properties obtained by illegal means and the possessions of terrorists pursuant to Section 14 of the AMLL. Further, an Investigation Body may also be formed by the Central Board to investigate the findings made in the report issued by the Scrutiny Body.

Chapter VIII of the AMLL sets out the anti-money laundering requirements on Reporting Organisations (as defined under the AMLL). Such requirements include the requirement to:

a) carry out risk assessments of money laundering and terrorism financing;

b) carry out intermediary measures on accounts, customers and business relationships;
c) monitor complex or unusually large transactions or transactions with a person from a country which does not follow measures to prevent money laundering and terrorism financing;
d) maintain records; and
e) implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing.

"Reporting Organisations" is defined under the AMLL to mean "*banks and financial institutions, non financial enterprises and professions stipulated by this Law to report. In this expression, it also includes organisations which is assigned to report, by notification from time to time by the Central Control Board*".

**(ii) Central Bank of Myanmar**

Specifically, for banks and financial institutions, Directive No. (21/2015) on CDD Measures dated 2 October 2015 ("Directive") issued by the Central Bank of Myanmar also applies.

The Directive sets out additional obligations on banks and financial institutions (which supplement the requirements as set out in Chapter VIII of the AMLL), and such anti-money laundering requirements include the requirement to:

a) implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing;
b) carry out risk assessment of money laundering and terrorism financing;
c) customer due diligence;
d) ongoing monitoring of customer transactions;
e) suspicious transaction reporting; and
f) recordkeeping.

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

We are not currently aware of any anti-money laundering requirements imposed by self-regulatory organisations or professional associations, to the extent they are publicly available.

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

The provisions of the AMLL are silent in this regard on the responsibility of the self-regulatory organisations or professional associations *vis-à-vis* their members. However, in general these self-regulatory organisations or professional associations do require that their members comply with all Myanmar laws (including the requirements and obligations under the AMLL) and may impose sanctions for failure to do so.

### 2.4 Are there requirements only at national level?

Yes, the requirements are only at national level and there are no specific state or regional level requirements.

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

Please see the responses to questions 1.4 and 2.1 above.

No, the criteria for examination are not publicly available.

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

Yes, the FIU is formed pursuant to the AMLL to investigate and prosecute offences under the AMLL.

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

There is no period of limitation for criminal offences in Myanmar.

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

Pursuant to Section 44 of the AMLL, failure to comply with the regulatory/administrative anti-money laundering requirements as listed in the response to question 2.1 above may attract a maximum penalty of imprisonment for a term which may extend to three years and may also be liable to a fine. If the offender is a company or organisation, K100 million shall be imposed on such company or organisation.

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

Please see the response to question 2.8 above which includes the maximum penalties of either imprisonment or fines under Chapter XI of the AMLL.

The other types of sanction are the confiscation orders or administrative orders that the Court is empowered to issue on properties and money relating to money laundering.

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

No, the penalties are not only administrative/civil.

The violation of anti-money laundering obligations is also subject to criminal sanctions under Chapter XI of the AMLL. Please see the response to question 2.8 above for more information.

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

There are no administrative decisions under the AMLL. In general under Myanmar law, administrative decisions are subject to appeal under the specific rules of that administrative body.

Under the AMLL, only the court is able to impose penalties/sanctions and such judgments by the courts are publicly available.

Yes, financial institutions are able to appeal against any penalty assessment rendered in judicial proceedings.

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

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

Reporting Organisations (as defined under the AMLL) are the entities subject to anti-money laundering requirements.

"Reporting Organisations" are defined under the AMLL to mean "*banks and financial institutions, non financial enterprises and professions stipulated by this Law to report. In this expression, it also includes organisations which is assigned to report, by notification from time to time by the Central Control Board*".

The non-financial enterprises and professions stipulated under the AMLL to be Reporting Organisations are as follows:

"*a) Casinos;*

*b) Real estate agents;*

*c) Dealers in precious metals and precious stones;*

*d) Lawyers, notaries, accountants or other independent legal professionals in respect of carrying out transactions acceptance and entrust of money and property of a client performing any of the following activities:*

- *a. buying and selling immovable property*
- *b. managing of client money, securities or other assets*
- *c. management of bank, savings or securities accounts*
- *d. organisation of contributions for the establishment, operation or management of companies*
- *e. establishment of legal societies or arrangements, operation or management of companies*

*e) Company, control body and company service providers which as a business provide any of the following services to third parties:*

- *a. acting as formation agent of legal persons*
- *b. acting as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal society or arrangement persons*
- *c. taking responsibility of a registration office, or business address, or correspondence or administrative address for a company, a partnership or any legal society arrangement*
- *d. acting as a trustee in a trusteeship company or performing the equivalent function in any legal society arrangement*
- *e. acting as a nominal shareholder or arranging a person to act as a nominal shareholder for another person.*"

Please see the answer to question 2.1 above for the obligations that Reporting Organisations are subject to.

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

We are not currently aware of any rules or regulations under Myanmar law which apply the anti-money laundering requirements to the cryptocurrency industry.

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

Yes, Reporting Organisations are required to implement internal programmes, policies, procedures and controls to combat money laundering and terrorism financing pursuant to Section 28 of the AMLL.

The required elements of such internal programmes, policies, procedures and controls are as follows:

"*a) intermediary measures, continuous focus investigation, monitoring the transactions, the obligations to report and to maintain the record;*

*b) supervising the procedures to ensure high standard of integrity of its service and a system to evaluate the personal, servicing and historical background of financial of these services;*

*c) continuous training programmes to assist by specific in respect of knowing their intermediary, recognising the specific responsibilities related to the anti money laundering and counter financial terrorism and transferring which are required to report contained in chapter 8;*

*d) an independent audit function to examine compliance with and effectiveness of the measures of taken action in implementing this Law.*"

Further, for banks and financial institutions, Clause 4 of the Directive is applicable and such internal programmes, policies, procedures and controls should address the following requirements:

"*a) Risk assessment of the customer as well as transactions;*

*b) Identification and verification of the customer, including walk-in/occasional customers, beneficial owners;*

*c) Application of customer due diligence measures to customers;*

*d) Exercising ongoing customer due diligence measures in relation to business relations and transactions;*

*e) Application of enhanced customer due diligence measures to high risk customers, including politically exposed persons;*

*f) Maintaining records and information of customers and transactions;*

*g) Monitoring transactions set out in section 21 of the AMLL;*

*h) Reporting to the Financial Intelligence Unit of transactions as set out in section 32 and 34 of the AMLL;*

*i) Ensuring that internal policies, procedures, systems and controls are subject to independent audit function and review;*

*j) The appointment of a compliance officer at senior management level to ensure compliance with the provisions of the AMLL, Rules issued the AMLL and the Directive;*

*k) Ensuring high standards of integrity while recruiting employees;*

*l) Providing an on-going training program to all new and existing employees, directors, board members and executive or management staff;*

*m) Other arrangements as prescribed by the CBM and competent regulatory authorities.*"

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

**Recordkeeping**

The requirements for such recordkeeping are as set out in Section 23 of the AMLL and Reporting Organisations are required to maintain records of the following:

"*a) evidence documents, records obtained from intermediary measure and finding documents including accounts and business correspondence of intermediary or beneficial owners for at least five years after the business relationship has been ceased or the occasional transaction has been carried out;*

*b) records on attemption of transaction in both domestic and foreign or records on transaction for the following five years after the transaction has been carried out;*

*c) copies of transaction reports under Chapter 8 of this law and other related documents for at least five years from the date of the report was submitted to the Financial Intelligence Unit; and*

*d) risk assessment and other underlying information for a period of five years from the date of its completion or update.*"

Further, for banks and financial institutions, Clause 58 of the Directive is applicable and copies of all records obtained through the customer due diligence process will need to be maintained.

**Reporting**

Section 32 of the AMLL provides that Reporting Organisations shall *promptly* report to the FIU if the amount of transaction is equal to or exceeds the designated threshold of US$10,000 or it has reasonable grounds to believe that any money or property is obtained by illegal means or is related to money laundering or terrorism financing or an attempt to do so. Please also note that Reporting Organisations are required to submit a suspicious transaction report to the FIU for suspicious transactions that may be an offence relating to money laundering or financing of terrorism. In addition, the FIU collects a wide range of transaction data (in addition to the aforementioned suspicious transactions report) including immovable property transactions, cash transactions and gems purchasing data from a wide range of Reporting Organisations. Despite the obligation to file these reports, only banks have filed suspicious transactions reports thus far, and threshold reports are rarely reported by other sectors.

Further for banks and financial institutions, Clause 47 of the Directive is applicable and a cross-border wire transfer in excess of US$10,000 or a domestic wire transfer in excess of K100 million will need to be reported to the FIU by either the ordering bank or beneficiary bank. Clause 49 of the Directive prescribes that banks or financial institutions should report to the FIU within 24 hours if they are situated in an urban area or within three days if they are situated in a remote area.

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

Reporting Organisations are required to submit a suspicious transaction report to the FIU for suspicious transactions that may be an offence relating to money laundering or financing of terrorism. Such suspicious transaction reports should be submitted to the FIU within 24 hours if the Organisation is situated in an urban area or within three days if it is situated in a remote area.

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

For banks and financial institutions, Clause 47 of the Directive is applicable and a cross-border wire transfer in excess of US$10,000 will need to be reported to the FIU by either the ordering bank or beneficiary bank. Clause 49 of the Directive prescribes that banks or financial institutions should report to the FIU within 24 hours if they are situated in an urban area or within three days if they are situated in a remote area.

This report should be in the form as prescribed under the AMLL as set out at Form 7 of the Anti Money Laundering Rules 2015.

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

Pursuant to Section 19(d) of the AMLL, Reporting Organisations are to undertake the following customer due diligence measures:

"*a) identifying the intermediary by means of free and reliable sources, documents, data or information and verifying the intermediary's registration;*

*b) Collecting and understanding the purpose of business relationship and the nature of information;*

*c) Identifying the main beneficiary to be verified that the reporting organizations may know who is the main beneficiary and understand possession and control of company or legal arrangement and taking the suitable measures in order to verify the evidence of the said beneficiary;*

*d) Verifying whether the person on behalf of intermediary is authorised person or not for person, company. organisation or legal arrangements and verifying the registration of that person is correct; verifying the legal status of person, company, organisation or legal arrangement; receiving information of intermediary's name, legal formation, address and directors and regulating the power to be bound to company or legal arrangements;*

*e) Enhancing customer due diligence measures contained in clauses (a) to (d) if it has reasonable grounds to believe that the customer is a domestic and foreign politically exposed person or international politically exposed person.*"

For banks and financial institutions, Clause 11 of the Directive is applicable and additional customer due diligence as follows would be required:

a) regarding natural persons, the Reporting Organisation must verify the identity of their customers using reliable, independent source documents, data, or information as outlined in Schedule 1 of the Directive; and

b) regarding legal persons or legal arrangements, the Reporting Organisation must obtain and verify the information required using reliable, independently sourced documents, data, or information as outlined in Schedule 1 of the Directive.

In brief, Schedule 1 of the Directive sets out certain specified information that banks and financial institutions would be required to collect from their customers.

Further, enhanced customer due diligence is required for higher risk customers as set out in Clause 17 of the Directive.

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

Clause 35 of the Directive provides that banks and financial institutions shall not enter into or continue a correspondent or business relationship with a shell bank or a correspondent financial institution in a foreign country that allows its accounts to be used by a shell bank.

**3.9 What is the criteria for reporting suspicious activity?**

There are no specified criteria but a suspicious transaction report is to be made if there are reasonable grounds to believe that a transaction or attempted transaction is money or property obtained by illegal means, or is related to money laundering or terrorism financing.

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

The Directorate of Investment and Company Administration, the registrar of companies in Myanmar, has set up an online registry, MyCo, which functions as a public registry of all companies and entities registered in Myanmar under the Myanmar Companies Law 2017. Information on shareholding and director appointment can be accessed on MyCo.

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

Yes, Clause 38 of the Directive prescribes that accurate originator and recipient information be included on the wire transfer.

Yes, such information should remain with the wire transfer and related messages throughout the payment chain.

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

Share certificates are *prima facie* evidence of the title of shares and the Myanmar Companies Law 2017 requires that a share certificate be issued to shareholders within 28 days of the allotment of shares.

A shareholder is recognised to be a shareholder of a company when such shareholder's name is indicated in the company's register of members.

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

Please see the answer to question 2.1 above.

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

No, as disclosed above, we are not currently aware of any anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones.

## 4 General

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

We are not currently aware of any additional anti-money laundering measures being contemplated or which are under consideration.

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

The last review conducted by the Asia/Pacific Group on Money Laundering from 20 November to 1 December 2017 stated that Myanmar is non-compliant with certain recommendations of the FATF, in particular on the following:

a) Recommendation 7 – Targeted Financial sanctions related to proliferation.
b) Recommendation 14 – Money or value transfer services.
c) Recommendation 19 – High-risk countries.
d) Recommendation 24 – Transparency and beneficial ownership of legal persons.
e) Recommendation 25 – Transparency and beneficial ownership of legal arrangements.
f) Recommendation 28 – Regulation and supervision of DNFBPs.

The above recommendations of the FATF do not currently form part of the AMLL and in order to comply with these recommendations, the main impediment would be having the legislative support to pass such legal reform.

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

The last review was conducted by the Asia/Pacific Group on Money Laundering from 20 November to 1 December 2017.

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

This can be obtained from the FIU website at https://mfiu. gov. mm/en.

English translations are available.

**Minn Naing Oo** is the Managing Director of Allen & Gledhill (Myanmar) and a Partner of Allen & Gledhill. He has extensive experience advising on banking and finance, mergers and acquisitions, infrastructure projects, corporate and commercial, arbitration and competition. He has acted for multinational corporations, multilateral agencies, financial institutions, private equity funds and Myanmar conglomerates.
He was previously the Chief Executive Officer of the Singapore International Arbitration Centre and Director at the Ministry of Trade and Industry Singapore. He is also a Fellow of the Chartered Institute of Arbitrators and the Singapore Institute of Arbitrators, and has been appointed to dispute panels for disputes between World Trade Organization (WTO) Member States.
Minn graduated from the National University of Singapore with an LL.B. in 1996. He was called to the Singapore Bar in 1997, and he obtained an LL.M. in 2001 from Columbia University as a Harlan Fiske Stone Scholar.

**Allen & Gledhill (Myanmar) Co., Ltd.**
Junction City Tower, #18-01
Bogyoke Aung San Road
Pabedan Township
Yangon
Myanmar

Tel: +95 1 925 3719
Email: minn.naingoo@allenandgledhill.com
URL: www.allenandgledhill.com/mm

**Dr. Ei Ei Khin** is a Consultant of Allen & Gledhill (Myanmar). Her experience focuses on commercial litigation and international arbitration. She has extensive research works and experience in commercial litigation, and advising on and being involved in various regulatory fields on behalf of the Supreme Court of the Union of Myanmar.
Prior to joining Allen & Gledhill (Myanmar), she was a Judicial Officer at the Supreme Court and a Judge at the township and district level of courts in Yangon and Mandalay, handling civil, criminal and juvenile cases. She was a head of office at the Office of the Chief Justice, High Court of Mandalay, and was also Deputy Director at the Supreme Court of the Union of Myanmar, where she was a member of the legal drafting committee of the Supreme Court and leader of the Working Group on the drafting of the new Arbitration Law, IP Laws and Insolvency Law.
She graduated from the University of Yangon with LL.B. and LL.M. degrees and holds a Ph.D. from Niigata University, Japan.

**Allen & Gledhill (Myanmar) Co., Ltd.**
Junction City Tower, #18-01
Bogyoke Aung San Road
Pabedan Township
Yangon
Myanmar

Tel: +95 1 925 3717/3718
Email: eiei.khin@allenandgledhill.com
URL: www.allenandgledhill.com/mm

Allen & Gledhill (Myanmar) is the local Myanmar office of one of South-east Asia's leading and largest law firms, Allen & Gledhill. Based in Yangon, we are a fully licensed law firm providing Myanmar legal and tax advice, and issues Myanmar legal opinions. Our Firm, staffed by local and foreign qualified lawyers, is supported by the network of Allen & Gledhill and combines sound local knowledge with best international practices to provide value-added advice and unparalleled service to our clients. The Firm is led by Minn Naing Oo, a Singapore- and New York-qualified lawyer fluent in the Myanmar language, who has well-established connections in the Myanmar business community and experience in advising both foreign investors and local businesses on their projects in Myanmar.
Operational since 2014, Allen & Gledhill (Myanmar) has gained an excellent reputation for advising local conglomerates and organisations as well as international clients across diversified industry sectors, and has been recognised as a leading law firm by notable legal directories including *IFLR1000*, *Chambers Asia-Pacific* and *The Legal 500 Asia Pacific*.

**www.allenandgledhill.com/mm**

ALLEN & GLEDHILL

# Netherlands

JahaeRaymakers


Jurjan Geertsma


Madelon Stevens



## 1 The Crime of Money Laundering and Criminal Enforcement

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

The Dutch Public Prosecution Service (**DPPS**, *Openbaar Ministerie*).

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

Under Dutch criminal law, the substantive standard can be generally described as the prohibition of conducting acts with regard to objects that – directly or indirectly – originate from a crime. According to Title XXXA of the Dutch Penal Code (**DPC**, *Wetboek van Strafrecht*), the prohibited acts are, amongst other things:

- Hiding or concealing:
  - the actual origin, finding place, disposal or transfer of the object; and
  - who the entitled person to an object is or who the person is that possesses the object.
- The acquisition, possession, transfer, conversion and use of an object that originates from a crime.

Please note that the term 'object' also covers property rights.

The DPC distinguishes the following types of money laundering:

- Intentional money laundering (Article 420*bis* DPC) (conditional intent regarding the origin of the object suffices).
- Habitual money laundering (Article 420*ter* DPC) (heaviest form, intentional money laundering on a regular basis).
- Money laundering as a regular occupation or business activity (Article 420*ter* DPC).
- Culpable money laundering (Article 420*quater* DPC) (lower limit, *culpa* regarding the origin of the object suffices).
- Simple money laundering (Article 420*bis* 1 and 420*quater* 1 DPC) (acquisition or possession of an object that originates directly from an own crime) (both the intentional and culpable form are criminalised).

The object that is being laundered must originate from a previous crime (*misdrijf*). It is not required that the object originates entirely from a crime: according to Dutch case law, an object that is also partly financed with criminal money and partly with legal money is considered to originate from a crime ("mixture"). Objects obtained through violations (*overtredingen*) fall outside the scope of money laundering under Dutch law.

Predicate offences can be all crimes whereby an object has been acquired, including tax evasion.

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

In general, the DPC provides jurisdiction for the DPPS to prosecute suspects for criminal offences if the case has a link with the Netherlands; for instance, if a Dutch person commits a crime abroad (as long as the act is punishable in the foreign country as well) or if the crime has been committed partially on Dutch territory.

In terms of jurisdiction, the DPC does not provide for a limitation in predicate offences. Therefore, the DPPS has jurisdiction to prosecute suspects for money laundering in the Netherlands of objects that originate from crimes committed and which are punishable abroad.

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

The DPPS, assisted by the Dutch police and Fiscal Intelligence and Investigation Service (**FIOD**).

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

According to Article 51 of the DPC, both individuals and legal entities are capable of committing criminal offences. It follows from Dutch case law that a legal entity can be held criminally liable for criminal offences of individuals (for instance, employees) if these offences can be 'reasonably attributed' to the legal entity, which depends on the specific facts and circumstances of the case. According to the Dutch Supreme Court, an important point of reference in this context is whether the offence (of the individual) took place within the 'sphere' of the legal entity.

Furthermore, according to Article 51 of the DPC, if criminal liability of the legal entity has been established, individuals that ordered the commission of the criminal offence (*opdrachtgever*) or actually directed the unlawful behaviour (*feitelijk leidinggever*) may also be prosecuted and convicted for such criminal offences.

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

Depending on the type of money laundering as discussed in question 1.2, the maximum penalties for individuals vary from:

- Imprisonment: three months (simple culpable money laundering) to eight years (habitual money laundering).
- Fines: EUR 21,750 to EUR 87,000.

The maximum penalties for legal entities (fines only) vary from EUR 87,000 to 10 per cent of the annual turnover of the previous fiscal year.

In addition, convicted individuals can be removed from (i) rights such as holding (certain) offices, serving with the armed forces, being counsel or judicial administrator, and (ii) the exercise of the profession in which the crime was committed (Article 420*quinquies* DCC).

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

According to Article 70 of the DPC, depending on the type of money laundering as discussed in question 1.2, the statute of limitations varies from six years (culpable money laundering and simple money laundering) to 20 years (habitual money laundering).

In addition, Article 72 of the DPC states that after any act of prosecution the statute of limitations starts over. The absolute statutes of limitations for the aforementioned money laundering crimes varies from 12 to 40 years (two times the initial statute of limitations).

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

In general, we see a development in which the cooperation between Dutch and foreign authorities in cross-border criminal cases increases. A more recent matter concerns the investigation of the DPPS to money laundering by the Dutch ING Bank in relation to corrupt payments made by telecom company VimpelCom to, amongst others, the daughter of the former president of Uzbekistan, Gulnara Karimova, for which the bank reached an out-of-court settlement with the DPPS.

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

The DPPS has the power to forfeit and confiscate objects.

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

We are familiar with a few cases in which (small) financial institutions or their directors have been convicted of money laundering. In addition, the DPPS seems to have increased its focus on so-called gate-keepers, especially large(r) financial institutions. For instance, in 2018 the DPPS conducted a criminal investigation to ING bank in relation to money laundering in the VimpelCom case. The bank reached a settlement with the DPPS for violation of the Money Laundering and Terrorist Financing (Prevention) Act (**Wwft**) and culpable money laundering. According to the DPPS, the bank did not prevent the bank accounts of ING customers in the Netherlands from being used to launder hundreds of millions of euros between 2010 and 2016. ING paid a fine of EUR 775,000,000.

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

In almost all large (international) fraud cases that have occurred so far, the DPPS has reached an out-of-court settlement (*transactie*) with suspects, in which settlements included the term of paying a certain fine.

The policy of the Dutch Public Prosecutors Office regarding high and special transactions ("*Aanwijzing hoge transacties en bijzondere transacties*") states that in principle a press release will be published for settlements of EUR 50,000 or more or special settlements between EUR 2,500 and EUR 50,000. Such a press release in any case includes the following information: a description of the criminal offences which according to the DPPS can be proven; a detailed prescription of the proposed settlement with respect to all involved suspects (specifically in case of a suspected legal entity and responsible individuals); a description of the underlying considerations with regards to the settlement (including a motivation of why the case should not be brought for a criminal judge); and an explanation of the amount of the fine.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

### 2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

Depending on the type of financial institution as mentioned in Article 1a Wwft, the authorities for imposing anti-money laundering requirements are:

- The Dutch Central Bank (**DNB**): regulator for banks; credit institutions; exchange institutions; electronic money institutions; payment institutions; life insurers; trust offices; and lessees of safes.
- The Dutch Authority for the Financial Markets (**AFM**): regulator for investment firms; investment institutions; and banks and financial service providers insofar as they mediate in life insurance policies and institutions for collective investment and securities (**UCITS**).
- The Financial Supervision Office (**BFT**): regulator for accountants; tax advisers; and notaries.
- The Dutch Tax Authority and Wwft Supervision Office: regulator for real estate agents or intermediaries; valuers; traders/sellers of goods; pawnshops; and domiciles.
- The local Dean of the Bar Association: the regulator for lawyers (attorneys-at-law).
- The Gaming Authority (**KSA**): regulator for gaming casinos.
- The investigation and enforcement services & intelligence and security services: Financial Intelligence Unit (authority

where institutions must report unusual transactions); and the DPPS (authority to investigate unusual transactions and other alleged criminal violations of the Wwft).

The Wwft comprises five core obligations:

- Taking measures to identify and assess its risks of money laundering and terrorist financing, including the recording of the results of such assessment. In addition, the obligation exists to have policies and procedures in place to mitigate and effectively manage the risks of money laundering and terrorist financing and the risks identified in the national and supranational risk assessment (Articles 1f–2d Wwft).
- Conducting a thorough – standard, simplified or strengthened – customer due diligence (**CDD**) prior to entering into a business relationship or conducting (incidental) transactions (Articles 3–11 Wwft).
- Reporting of unusual transactions with the Financial Intelligence Unit, on the basis of objective or subjective indicators (Articles 12–23a Wwft).
- Providing periodic training to employees in order for them to be able to recognise unusual transactions and conduct a proper and comprehensive CDD (Article 35 Wwft).
- Adequate record-keeping of risk assessment/CDD and reporting of unusual transactions and providing these results to regulators upon request (Articles 33–34 Wwft).

### 2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Most of the authorities mentioned in question 2.1 (of which some are self-regulatory organisations such as the local Dean of the Bar Association) provide guidelines for the Wwft institutions in order to assist them in complying with the obligations of the Wwft. However, the authorities do not impose additional requirements.

### 2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The authorities mentioned in question 2.1 are responsible for anti-money laundering compliance and enforcement against the Wwft institutions that fall under their responsibility.

### 2.4 Are there requirements only at national level?

Since the Wwft obligations are implementations of the requirements as set by the European AML Directives, the Wwft obligations stem from international level. For instance, the FATF standards are relevant in this regard.

### 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

Please see questions 2.1 and 2.2. Please note that the guidance provided is not always up to date or very clear. For example, the general guidance dates January 2014, although since the end of 2019 a new version has been 'in consultation'.

### 2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

According to the Wwft, the Dutch Financial Intelligence Unit (http://www.fiu-nederland.nl) is the only and central reporting point where the Wwft institutions must report unusual transactions.

### 2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Enforcement of the Wwft can take place via administrative measures, such as an order subject to an incremental penalty (*last onder dwangsom*) in order to stop the institution of violating the Wwft or an administrative penalty (*bestuurlijke boete*). The statute of limitations for an administrative penalty is five years from the day of the violation.

In addition, violation of (one or more of) the five core obligations as discussed in question 2.1 can constitute a criminal offence under the Economic Crimes Act (WED, *Wet op de economische delicten*) for which the DPPS can start prosecution. According to Articles 1, 2 and 6 of the WED in conjunction with Articles 70 and 72 of the DPC, the absolute statutes of limitations vary from six years (in the case of a culpable violation) to 24 years (in the case of a habitual and intentional violation).

### 2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Administrative penalties: for most violations of the aforementioned five core obligations of the Wwft, the assigned regulator can impose administrative penalties that may vary from EUR 10,000 (minor violation) to EUR 4,000,000 (serious violation). The maximum penalty for banks, trust offices and a few other financial institutions such as investment firms amounts to EUR 5,000,000. In case of recidivism within five years from a previous violation, the administrative penalty can be twice the aforementioned amounts. In addition, in case of serious violations by banks, trust offices and a few other financial institutions, the Wwft provides for administrative penalties of up to 20 per cent of the net turnover of the previous fiscal year.

Criminal penalties: the maximum penalties for violations of the aforementioned five core obligations of the Wwft vary from six months to four years' imprisonment or fines ranging from EUR 21,750 to EUR 87,000 for natural persons. The maximum penalties for legal entities (fines only) vary from EUR 87,000 to 10 per cent of the annual turnover of the previous fiscal year. In addition, the WED prescribes that if the value of the goods with which or with regard to which the crime has been committed, or which has been wholly or partly obtained through the crime, is higher than the fourth part of the maximum of the fine which can be imposed, a fine of the next higher category may be imposed.

### 2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The WED in conjunction with the DPC can impose various additional penalties (*bijkomende straffen*) such as removal from holding offices for a certain period and total or partial cessation of the

entity of the convicted person where the crime was committed. In addition, certain measures (*maatregelen*) can be imposed, such as deprivation of the unlawfully obtained advantage.

In addition, the Wwft provides for the obligation of regulators to publish administrative fines in certain cases.

**2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?**

Please see the answers to questions 2.8 and 2.9 above.

**2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?**

Judicial proceedings in the Netherlands are public.

If an institution gets convicted of criminal violations of the DPC or Wwft by a District Court, it can appeal such verdict to the Court of Appeal. In case of a conviction by the Court of Appeal in criminal proceedings, an institution can under certain circumstances appeal to the Supreme Court, which has the competence to set aside or affirm rulings of lower courts, but no competence to re-examine or question the facts. The Supreme Court only considers whether the lower courts applied the law correctly and the rulings have sufficient reasoning.

In administrative proceedings, an institution must first file a complaint (*bezwaar*) with the administrative body imposing the sanction, followed by an appeal before the court. Under certain circumstances, a possibility to appeal against a ruling by the court with the Commission for Appeal for business and industry exists.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

Article 1a Wwft distinguishes three main categories of "institutions", namely:

1) Banks.
2) Other financial institutions:
   a) Investment institutions.
   b) Investment firms.
   c) Mediators in life insurance.
   d) Payment service agents.
   e) Payment service providers acting on behalf of a payment service provider with another EU Member State licence.
   f) Payment service providers.
   g) Electronic money institutions.
   h) UCITS.
   i) Institutions not being a bank that nevertheless carries out banking activities.
   j) Life insurers.
   k) Landlords of safes.
   l) Currency exchange offices.
3) Designated natural persons or legal entities acting in the context of their professional activities:
   a) Accountants.
   b) Lawyers.
   c) Tax advisers.
   d) Domicile providers.
   e) Traders/sellers of real estate, vehicles, ships, art objects, antiques, precious stones, precious metals, or jewellery.
   f) Brokers or intermediaries in matters of great value (EUR 10,000 or more).
   g) Notaries.
   h) Pawnshops.
   i) Gaming casinos.
   j) Appraisers.
   k) Trust offices.

With regard to lawyers and (junior) notaries, the Wwft is only applicable if they:

1) independently provide professional or professional advice or assistance with:
   i) the purchase or sale of registered goods;
   ii) managing money, securities, coins, notes, precious metals, precious stones or other values;
   iii) the establishment or management of companies, legal persons or similar bodies as referred to in Article 2, first paragraph, part b, of the General Government Tax Act;
   iv) the purchase or sale of shares in, or the total or partial purchase or sale or takeover of companies, companies, legal persons or similar bodies as referred to in Article 2, first paragraph, under b, of the General Government Tax Act;
   v) activities in the field of taxation that are comparable to the activities of the professional groups described in part a; and
   vi) establishing a mortgage right on registered property; or
2) act independently, professionally, or commercially in the name and on behalf of a client in any financial transaction or real estate transaction.

The Wwft does not apply to tax advisers, lawyers and notaries, in so far as they perform work for a client regarding the determination of his legal position, his legal representation and defence, giving advice before, during and after legal proceedings, or giving advice on instituting or avoiding legal proceedings.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

In line with the Fourth Anti-Money Laundering Directive, a legislative proposal is currently pending to bring virtual currency under the scope of the Wwft. In April 2020, this is pending at the Senate. We expect this to enter into force over the course of 2020.

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

As discussed in question 2.1, the Wwft comprises five core obligations that Wwft institutions are required to meet. It is up to the institutions themselves to decide on how they implement such obligations. Dutch law does not provide for an obligation to maintain specific compliance programmes.

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

Recordkeeping: a Wwft institution has to keep records of:

- the performed client due diligence on the basis of the Wwft; and
- the measures it took to investigate complex and unusually large transactions.

Article 33 Wwft states that the institution must keep these records for five years from the date of termination of the business relationship or the date the transaction has been executed.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

According to Article 16 of the Wwft, an institution is obliged to immediately (but in any case within two weeks) report an unusual intended or effected transaction with the FIU, right after it became aware of the unusual nature of the transaction. The reporting obligation also applies if:

- a CDD failed and there are also indications that the customer concerned is involved in money laundering or terrorist financing; or
- a business relationship is terminated and there are also indications that the customer concerned is involved in money laundering or terrorist financing.

In order to determine the nature of the transaction, the Uitvoeringsbesluit Wwft 2018 provides for objective and subjective indicators for specific Wwft institutions. Objective indicators for banks and some other financial institutions are, for instance, (cash) transactions of EUR 10,000 or more or money transfer of EUR 2,000 or more. Subjective indicators are more vague. A frequently used subjective indicator is, for instance, if a transaction gives reason for the institution to assume that it may be related to money laundering or terrorist financing.

**3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?**

Though Dutch law is not very clear on this point, the Wwft does not seem to provide for a territorial delineation of unusual transactions as such. The parliamentary history of the Wwft and Dutch caselaw seem to suggest that foreign transactions may also be subject to the reporting requirements of Article 16 Wwft. Therefore, Wwft institutions can also be obliged to report cross-border transactions, if such transactions are considered to be unusual, as discussed in question 3.5.

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

As discussed in question 2.1, the Wwft provides for three types of CDD: standard; simplified; or strengthened CDD. All types of due diligence need to be conducted prior to entering into a business relationship or conducting (incidental) transactions (Articles 3–11 Wwft).

The type of CDD an institution needs to conduct in a specific case entirely depends on the type of client and transaction. The starting point is that an institution conducts a standard CDD, unless a business relationship or transaction by its nature entails a low risk of money laundering or financing of terrorism. In that case, a simplified due diligence suffices. If a business relationship or transaction by its nature entails a high risk of money laundering or financing of terrorism, the institution must conduct a strengthened due diligence. This is also the case if the state where the customer is domiciled or established or has its seat has been designated by the European Commission as a state with a higher risk of money laundering or terrorist financing on the basis of Article 9 of the Fourth Anti-Money Laundering Directive.

Where a risk on money laundering or financing of terrorism in a specific case exists, a background check of the customer, identification of the Ultimate Beneficial Owners (**UBOs**) and the purpose and nature of the business relationship, amongst others, will also need to be determined.

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

According to Article 5 Wwft, it is prohibited for banks and other financial institutions to enter into or continue a correspondent relationship with a shell bank or with a bank or other financial institution that is known to allow a shell bank to use its accounts.

**3.9 What is the criteria for reporting suspicious activity?**

Please see question 3.5. Please note that in the Netherlands unusual activities should be reported.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

As of March 2019, the Netherlands has still not fully implemented the Fourth Anti-Money Laundering Directive. Consequently, there is no register for UBOs to date.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

We refer to the DNB guidance that describes the following:

FATF Special Recommendation VII on wire transfers stipulates that electronic transfers must contain certain information about the party instructing the payment. In Europe, this FATF Recommendation has been transposed into Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying the transfer of funds. The Regulation has direct effect in the Netherlands. The Wwft stipulates that a customer due diligence

must be performed whenever an institution effects a non-recurring transaction into or out of the Netherlands on behalf of a customer or a trust that involves a transfer of funds as referred to in Section 2(7) of the Regulation.

The Regulation lays down rules concerning the information on the payer that must accompany the transfer of funds in order to ensure that the authorities responsible for combatting money laundering and terrorist financing have direct access to basic information that can help them exercise their duties. Institutions will generally have access to this information from the customer due diligence. The institution also performs a customer due diligence when executing a non-recurring transaction into or out of the Netherlands on behalf of a customer or trust which is effecting a transfer of funds.

Full information about the payer comprises:

- Name.
- Address (or date and place of birth, customer identification number or national identity number).
- Account number (if this is not available, replace it with a unique identification code that can be used to trace the payer).

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

Please note that in 2019 a law entered into force that decided that the issuing of bearer shares can only be done via a global certificate that will be filed at the central institute or an intermediary. All bearer shares not filed at the central institute or an intermediary should have been converted to registered shares in 2019. From 2020, all bearer shares that have not been converted will automatically be converted to registered shares. Anonymous transfer of bearer shares is no longer possible.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

Yes, we refer to the list provided in question 3.1 which describes that non-financial institutions are also considered to be Wwft institutions to which the Wwft core obligations apply; for instance, natural persons or legal entities acting in the context of their professional activities:

a) traders/sellers of real estate, vehicles, ships, art objects, antiques, precious stones, precious metals, or jewellery; and
b) brokers or intermediaries in matters of great value (EUR 10,000 or more).

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

Please see question 3.13 above.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

A part of the Fourth Anti-Money Laundering Directive still has to be implemented. The Fifth Anti-Money Laundering Directive still has to be implemented in whole.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

Please see question 4.1 above. The last FATF evaluation is from 2014 and therefore is no longer up to date.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The FATF has evaluated the anti-money laundering regime of the Netherlands. For further information please see: http://www.fatf-gafi.org/documents/documents/fur-netherlands-2014.html.

**4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?**

For English publications we refer to:

- The website of the FIU: https://www.fiu-nederland.nl/en.
- DNB Guidance on the Wwft: http://www.toezicht.dnb.nl/en/ bin aries/51-212353.pdf.
- The Fifth European Anti-Money Laundering Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A3 2018L0843.

**Jurjan Geertsma**'s legal practice focuses expressly on disciplinary law, the law of sanctions and the reputational issues involved. He helps his clients to identify potential risks, jointly draws up an appropriate strategy, and proactively and resolutely goes in search of solutions. He assists companies from a wide range of sectors (including the chemical, food and property sectors), financial institutions (such as trust offices) and professional practitioners (e.g., the healthcare sector and the notarial and accountancy practices) who are faced with criminal accusations, administrative enforcement, and supervisory and disciplinary issues. Jurjan is a member of the Dutch Association of Defence Counsel (**NVSA**) and the European Criminal Bar Association (**ECBA**), where he forms part of the Anti-Corruption Working Group. He is also involved in the Corporate Responsibility & Anti-Corruption Commission of the International Chamber of Commerce (**ICC**), and the Asset Tracing & Recovery working group of the Institute for Financial Crime (**IFFC**). He teaches courses at institutions, for professional practitioners and for legal and compliance officers in the fields of Anti-Money Laundering (**AML**), Anti-Bribery & Corruption (**ABC**), International Sanctions Regulations and Compliance, Integrity, Client Confidentiality and Lawyer-Client Privilege, and organises interrogation and search ('mock dawn raid') training sessions.

**JahaeRaymakers**
Mondriaantoren, 19th floor
Amstelplein 40
1096 BC Amsterdam
Netherlands

Tel: +31 20 435 25 25
Email: geertsma@jahae.nl
URL: www.jahae.nl

**Madelon Stevens** is specialised in financial, economic and tax sanctions law. She advises and provides assistance to companies and individuals who, as suspects, witnesses or victims, are at risk of becoming involved in administrative or criminal supervision or enforcement issues, related to compliance with environmental and labour legislation (industrial accidents), corruption, (tax) fraud, forgery and money laundering. She also provides training, including how to act in an investigation/raid by supervisors or investigative authorities.
In addition, Madelon is specialised in anti-corruption issues. She advises and assists clients in developing anti-corruption policies and training programmes and conducting an internal investigation if there is reason to do so. In this context, Madelon also advises on taking appropriate follow-up steps, such as the advantages and disadvantages of self-reporting with the authorities. Madelon also regularly publishes updates on relevant developments in this area.
Madelon is a member of the Dutch Association of Young Criminal Lawyers (**NVJSA**) and the Women's White Collar Defense Association (**WWCDA**).

**JahaeRaymakers**
Mondriaantoren, 19th floor
Amstelplein 40
1096 BC Amsterdam
Netherlands

Tel: +31 20 435 25 25
Email: stevens@jahae.nl
URL: www.jahae.nl

JahaeRaymakers is a leading niche firm with 10 lawyers. The firm specialises in risk & reputation management, supervision & enforcement, law of sanctions and European & international proceedings. Its lawyers act as trusted advisors for a wide range of public authorities, (listed) companies, museums and their directors, and high-profile and other private individuals. They have detailed knowledge, a wealth of experience and an excellent international network.
Trust, discretion, quality and determination are paramount in the often sensitive cases handled by JahaeRaymakers. The firm's aim is to adequately solve all cases. Whenever possible, it looks to take action before problems occur, preferably in the background and out of court. Where necessary, the firm does battle in court to achieve the best possible outcome for all its clients.

**www.jahae.nl**

# Poland


Wojciech Kapica

Magdalena Jaczewska

SMM Legal Maciak Mataczyński


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

In Poland, money laundering is prosecuted by the public prosecutor's offices. Regional Prosecutor's Offices conduct and supervise the penal proceedings in criminal cases connected with the most serious criminal, financial and tax offences. Investigations are conducted either by public prosecutors or by the local police.

### 1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Article 299 of the Polish Criminal Code states that anyone who receives, transfers or transports abroad, or assists in the transfer of title or possession of legal tender, securities or other foreign currency values, property rights or real or movable property obtained from the profits of offences committed by other people, or takes any other action that may prevent or significantly hinder the determination of their criminal origin or place of location, their detection or forfeiture, is liable to imprisonment of between six months to eight years. Moreover, anyone who as an employee of a bank, financial or credit institution, or any other entity legally obliged to register transactions and the people performing them, unlawfully receives a cash amount of money or foreign currency, or who transfers or converts it, or receives it under other circumstances raising a justified suspicion as to its origin from the offences specified above, or who provides services aimed at concealing its criminal origin or in securing it against forfeiture, is liable to the penalty specified above. If the offender commits an act specified above acting in concert with other people, he or she is liable to imprisonment of between one to 10 years.

Tax evasion is not a predicate offence for money laundering. Tax evasion is an offence according to the Polish Penal Fiscal Code.

### 1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

In principle, according to Article 5 of the Polish Criminal Code, Polish criminal law applies to an offender who commits a prohibited act in the Republic of Poland, or on a Polish vessel or aircraft, unless the Republic of Poland is a party to an international agreement stating otherwise.

In addition, the Polish Criminal Code applies also to Polish citizens who have committed an offence abroad (Article 109 of the Polish Criminal Code) as well as to foreigners who have committed a prohibited act abroad that is against the interest of the Republic of Poland, a Polish citizen, a Polish legal entity or a Polish organisational unit without the status of a legal entity. Moreover, Polish criminal law applies to foreigners who have committed a prohibited act abroad other than acts mentioned above, if, under Polish criminal law, the prohibited act is subject to a penalty exceeding two years' imprisonment, where the offender is in the Republic of Poland and where no decision on his or her extradition has been taken.

For an act committed abroad to be considered an offence, it must be considered an offence by the law in force where it was committed (Article 111 § 1 of the Polish Criminal Code).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The public prosecutor's offices are responsible for investigating and prosecuting. Investigations might also be conducted by the local police.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

Polish criminal law applies only to natural persons. However, the so-called collective entities bear liability for acts prohibited under penalty as offences or fiscal offences according to rules stated in the Act of 28 October 2002 on the Liability of Collective Entities for Acts Prohibited Under Penalty (hereinafter referred to as "the Act").

Pursuant to Article 2 of the Act, a collective entity is a legal person and organisational unit without legal personality on which separate laws and regulations confer legal capacity, except for the State Treasury, local governments units and their unions. A collective entity according to the Act is also a commercial company with the shareholding of the State Treasury as well as a company with the shareholding of local governments units or union of such units, a company in organisation, an entity in liquidation, an entrepreneur not being a natural person, and a foreign organisational unit.

According to the Act, a collective entity may hold responsibility for, *inter alia*, all offences related to economic activity,

penal and fiscal offences, public corruption and corruption in business, including the crime of money laundering.

A collective entity bears liability for the prohibited act committed by a natural person if such behaviour brought or might have brought some benefit to a collective entity (even immaterial). A collective entity bears such liability if the person:

- acts on behalf of or in the interest of the collective entity within the scope of power or duty to represent it, makes decisions on its behalf or exercises internal control, or in having exceeded such power or failed to perform this duty;
- was permitted to act as a result of having exceeded powers or failed to perform the duties by the person referred to above; and
- acts on behalf of or in the interest of the collective entity, with the consent or knowledge of the person referred to above.

According to Article 4 of the Act, the collective entity bears liability if the fact of committing the prohibited act by the person mentioned above has been approved by a valid judgment convicting such person, a decision on conditional discontinuance of penal proceedings or proceedings in the case involving a fiscal offence in respect of such person, or if a decision permitting such person to voluntarily accept the liability or a court decision on discontinuance of proceeding against such person due to a circumstance excluding the punishment of the perpetrator.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Money laundering is punishable by imprisonment of between six months to eight years. However, if the offender commits the act of money laundering acting in concert with other people as well as in the case where the offender gains significant material benefit, he or she is liable to imprisonment of between one to 10 years.

In reference to collective entities, the court adjudicates a monetary penalty of an amount between PLN 1,000 and PLN 5,000,000; however, the penalty must not exceed 3% of the revenue earned in the financial year in which the prohibited act forming the grounds for liability of the collective entity was committed.

In respect of collective entities, the court should also decide the forfeiture of the following:

- objects coming, even indirectly, from the prohibited act or objects which served or were designed for committing the prohibited act;
- material benefit coming, even indirectly, from the prohibited act; and
- the value equivalent to the value of objects or material benefits coming, even indirectly, from the prohibited act.

Apart from what is stated above, the following may be adjudicated in respect of collective entities:

- prohibition of promotion or advertising of the conducted activity, manufactured or sold products and provided services or performances;
- prohibition of benefitting from grants, subventions or other forms of financial support involving public funds;
- prohibition of benefitting from assistance of international organisations of which the Republic of Poland is a member;
- prohibition of bidding for public contracts; and
- making the judgment publicly known.

The abovementioned prohibitions are adjudicated for a period of between one year and five years.

### 1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations for money laundering is 15 years from the moment the offence was committed (Article 101 § 1 point 2a of the Polish Criminal Code).

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

There are no parallel state or provincial criminal offences in Poland.

### 1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

According to the Polish Criminal Code, in the case of criminal conviction for money laundering, the court orders the forfeiture of items derived either directly or indirectly from the offence, or the gains of the offence, or an equivalent value, even if they are not the property of the offender. Forfeiture is not ordered if all or part of the gains, or their equivalent, are returned to the aggrieved party or another entity.

The Polish Criminal Code provides for the possibility of forfeiture if there is no criminal conviction. Pursuant to Article 45a of the Polish Criminal Code, the court may order the forfeiture in the case where the effects of a prohibited act on society are insignificant, as well as in the case where the court conditionally discontinued criminal proceedings or if the offender has committed a prohibited act in a state of unaccountability or if there are circumstances excluding punishment.

Apart from the above, if evidence collected during proceedings show that in the case of conviction, the forfeiture would be ordered, the court may also order forfeiture in the following situations:

- in the event of the death of the offender;
- in the event of discontinuation of criminal proceedings because of the failure to identify the offender;
- in the event of suspension of criminal proceedings; or
- if the accused cannot take part in the proceeding because of mental disorder or other dread disease.

For forfeiture concerning collective entities, please see question 1.6 above.

### 1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

There are no widely known cases of banks or other financial institutions or their directors, officers or employees having been convicted of money laundering in Poland. However, such cases may have taken place.

### 1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

According to the Polish Code of Criminal Procedure, there is a possibility to refrain from further actions if the accused pleads guilty and in the view of his or her explanations, the

circumstances of the offence and the guilt of the accused do not raise doubts and the attitude of the accused indicates that the purposes of the proceedings will be achieved. In such case, the public prosecutor, instead of indictment, files with the court a motion to issue a sentence of conviction and imposition on the accused of a penalty or a penal measure agreed with him or her, applicable to summary offence, with which the accused is charged. Arrangements conducted between the public prosecutor and the accused should be reflected in the abovementioned motion.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

**2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.**

The following authorities of government administration are competent for the matters of anti-money laundering and terrorist financing:

1) the minister competent for public finance as the supreme financial authority; and
2) the General Inspector of Financial Information (Polish Financial Intelligence Analysis Unit).

Furthermore, for financial institutions there is also scope of AML supervision provided by the Polish Financial Supervision Authority ("KNF").

**2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?**

There are no money-laundering requirements imposed by self-regulatory organisations or professional associations. Lawyers, notaries and tax advisers are obliged to respect the requirements imposed by the Act of 1 March 2018 on Counteracting Money Laundering and the Financing of Terrorism (hereinafter referred to as the "Polish Act").

**2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?**

No, the authorities listed above in question 2.1 are competent for anti-money laundering compliance and enforcement against members of self-regulatory organisations and professional associations in the scope of the Polish Act.

**2.4 Are there requirements only at national level?**

Money-laundering requirements are codified in the Polish Act. Apart from that, as a member of the European Union, Poland should also respect European regulations and guidelines in this matter.

**2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?**

The General Inspector of Financial Information is responsible for the examination of compliance and enforcement of anti-money laundering requirements. According to the Polish Act, the General Inspector of Financial Information in the scope of his tasks carries out activities with a view to counteracting money laundering and terrorist financing; in particular, the General Inspector of Financial Information is, *inter alia*, exercising control over compliance with the provisions on counteracting money laundering and terrorist financing, handing over to the entitled authorities information and documents substantiating suspicion of committing an offence, as well as conducting the procedure of suspension of a transaction or blocking an account, and demanding the provision of information on the transaction and making it publicly available.

Additionally, as part of the exercised supervision or conducted inspection, the inspection is also conducted by:

- the President of the National Bank of Poland – with regard to the entities carrying out exchange bureau activity;
- the Polish Financial Supervision Authority – with regard to obliged institutions supervised by the Authority;
- the National Cooperative Savings and Credit Fund – with regard to cooperative savings and credit funds;
- presidents of courts of appeal – with regard to notaries;
- heads of customs and revenue offices – with regard to the obliged institutions supervised by those authorities;
- province governors and district heads – with regard to associations; and
- ministers and district heads – with regard to foundations.

On 17 July 2019, the General Inspector of Financial Information published the first version of the National Risk Assessment with its proper attachments. The document can be treated as some form of publicly available examination criteria in conjunction with AML regulations.

**2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?**

In Poland, the General Inspector of Financial Information as the FIU, *inter alia*, analyses information on property values which the General Inspector of Financial Information suspects are linked with an offence of money laundering or terrorist financing.

**2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?**

With regard to money laundering, competent authorities according to Article 189 g of the Polish Act of Administrative Proceeding cannot impose an administrative monetary penalty if a period of five years has elapsed since the infringement of law or occurrence of the effects thereof. Moreover, the administrative monetary penalty is not subject to enforcement after five years from the day on which the sanction should have been enforced has passed.

**2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?**

In principle, the monetary penalty imposed for failure to comply with the regulatory/administrative anti-money laundering requirements

may be up to twice the amount of the profit gained or loss avoided by an obliged institution as a result of a violation, or – where determining the amount of this profit or loss is not possible – up to the amount of the equivalent of EUR 1,000,000.

Additionally, the monetary penalty against, *inter alia*, banks, investment firms or foreign legal persons carrying out brokerage activity on the territory of Poland may have a fine of up to PLN 20,868,500 imposed in the case of natural persons, and – in case of the legal person or an organisational unit having no legal personality – up to the amount of the equivalent of EUR 5,000,000 or up to 10% of the turnover reported in the last approved financial statements for a financial year or in the last consolidated financial statements for a financial year – in the case of institutions covered by the consolidated financial statements of a capital group.

There are various failures that are subject to the penalty provisions, such as the:

- failure to discharge the obligation of appointment of a person responsible for the fulfilment of the obligations laid down in the Polish Act;
- failure to discharge the obligation of ensuring that the transfer of funds is accompanied by information on the payer or the recipient;
- failure to discharge the obligation of implementing effective procedures that enable the detection of missing information on the payer or the recipient;
- failure to discharge the obligation of freezing funds or economic resources or the prohibition of making the funds or economic resources available; and/or
- failure to discharge the obligation of application-specific restrictive measures.

**2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?**

Besides monetary penalties, the following penalties may be imposed on obliged institutions:

- the publication of the information about an obliged institution and the extent of their violation of the provisions of the Polish Act in the official publication on a dedicated website of the office providing support for the minister competent for public finance (Pol. *Biuletyn Informacji Publicznej*);
- the order to cease to undertake specific acts by an obliged institution;
- withdrawal of a concession or permission or removal from the register of a regulated activity; and
- the prohibition of discharging duties at an executive post by the person liable for the obliged institution's violation of the provisions of the Polish Act, for a period not exceeding one year.

**2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?**

No, there are also criminal sanctions for violation of anti-money laundering obligations. The following violations are subject to criminal sanction according to Article 156 of the Polish Act:

- failure to discharge the obligation of providing to the General Inspector of Financial Information a notification about the circumstances that may imply a suspicion of commission of the offence of money laundering or terrorist financing, or the obligation of providing to the General Inspector of Financial Information a notification of the arising of a substantiated suspicion that a specific transaction, or property values being the subject of this transaction, could be linked to money laundering or terrorism financing;
- providing or concealing to the General Inspector of Financial Information inaccurate data concerning transactions, amounts or persons; and
- disclosing to unauthorised persons, account holders or the persons to whom a transaction refers the information gathered pursuant to the Polish Act, or making use of this information at variance with the provisions of the Polish Act.

In the abovementioned case, the person who commits the act is liable to imprisonment of between three months to five years.

The Polish Act also penalises the thwarting or hindering of an inspection with a fine (Article 157 of the Polish Act).

**2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?**

The process for assessment and collection of sanctions and appeal of administrative decision is as follows:

Firstly, the competent authority (the General Inspector of Financial Information, the President of the National Bank of Poland or the Polish Financial Supervision Authority) issues a decision.

In the case where the decision was issued by the General Inspector of Financial Information, the obliged institution may submit a complaint to the Provincial Administrative Court within 30 days from the delivery of the decision.

In the case where the decision was issued by the President of the National Bank of Poland, the obliged institution may submit a motion for reconsideration. After exhaustion of the abovementioned remedies, the obliged institution may submit a complaint to the Provincial Administrative Court within 30 days from the delivery of the decision. The same procedure applies to the decisions issued by the Polish Financial Supervision Authority.

The General Inspector of Financial Information posts the information on a dedicated website of the office providing support for the minister competent for public finance (Pol. *Biuletyn Informacji Publicznej*), regarding:

- the issuance of the final decision imposing an administrative penalty;
- the lodging of a complaint against such decision; and
- the decision taken as a result of examining the abovementioned complaint.

Such information includes identification data of obliged institutions on which the administrative penalty was imposed, the type and nature of violation of the provisions, as well as the type of amount of the imposed administrative penalty.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

The Polish Act applies to the following entities acting in the course of business in Poland:

- domestic banks, branches of foreign banks, credit banks and financial institutions;
- investment funds, alternative investment companies, investment fund corporations;
- payment institutions and electronic money institutions;
- investment firms;
- foreign legal persons conducting brokerage activity within the territory of the Republic of Poland, including those conducting such activity in a form of a branch, and commodity brokerage houses;
- companies operating a regulated market within the scope of the operation of the auction platform;
- insurance undertakings in selected cases and insurance intermediaries;
- Krajowy Depozyt Papierów Wartościowych S.A. (National Securities Deposit) and a company to which Krajowy Depozyt Papierów Wartościowych S.A. has delegated activities;
- entrepreneurs conducting exchange office activity and other entrepreneurs providing a foreign exchange service or a foreign exchange intermediation service;
- entities conducting economic activity consisting of providing services in the area of exchange between virtual currencies and means of payment, intermediation in the exchange referred, the operation of the accounts referred in this regard;
- notaries, attorneys, legal counsels, foreign lawyers and tax advisors in certain cases;
- entrepreneurs in certain cases (*inter alia*, establishment of legal person, providing a registered office);
- entities conducting activity in the area of the provision of bookkeeping services;
- real estate agents;
- postal operators;
- entities conducting activity in the area of games of chance, betting, card games, and machine games;
- foundations and associations in selected cases; and
- lending institutions.

The Polish Act requires obliged institutions to identify and assess the risks associated with money laundering and terrorism financing, implement and apply the financial security measures proportional to the risk identified during customer analysis, gather and transfer to the appropriate institutions information provided for by law, conduct training, cooperate with the General Inspector of Financial Information in the event of suspicion of money laundering or financing of terrorism and implement the organisational activities aimed at ensuring proper implementation of basic tasks of obliged institutions.

### 3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

The institutions that have been added to the catalogue of obliged institutions are the entities conducting economic activity consisting of providing services in the area of exchange between virtual currencies and means of payment, exchange between virtual currencies, intermediation in the exchange and the operation of the accounts. The definition of virtual currencies was introduced.

### 3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All obliged institutions are required to implement an internal anti-money laundering and terrorist financing procedure, which must contain the elements indicated in Article 50 sec. 2 Polish Act. These include, *inter alia*:

1) activities or actions taken in order to mitigate any money laundering and terrorist financing risks and to manage appropriately the money laundering or terrorist financing risks identified;
2) rules for identifying and assessing money laundering and terrorist financing risks involved in a given business relationship or occasional transaction;
3) measures applied to manage appropriately the identified money laundering or terrorist financing risk involved in a given business relationship or occasional transaction; and
4) the rules for fulfilling obligations including the provision of information on transactions and notifications to the General Inspector of Financial Information.

Furthermore, in the procedures set out above there are also rules for the reporting of actual or potential breaches of provisions on counteracting money laundering and terrorist financing by employees. This is an additional measure to ensure compliance with the law. The abovementioned measures are to ensure obligations comply with AML.

### 3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

The Polish Act does not distinguish specific requirements for recordkeeping or reporting large currency transactions. In this respect, general requirements are applied.

### 3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Apart from exceptions stated in question 3.6 below, transactions in an amount of the equivalent of EUR 15,000 or a cash payment in an amount exceeding the equivalent of EUR 10,000 should be reported when received.

### 3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

In accordance with Article 72 sec. 2 of the Polish Act, the obliged institutions (with exceptions) shall provide the General Inspector with information on an executed transfer of funds for an amount exceeding the equivalent of EUR 15,000, except for:

1) a transfer of funds between a payment account and a term deposit account that belong to the same customer in the same obliged institution;
2) a domestic transfer of funds from another obliged institution;
3) a transaction related to the obliged institution's own operations, carried out by the obliged institution in its own name and on its own behalf, including a transaction concluded on the interbank market;
4) a transaction carried out in the name or on behalf of the units of the public finance sector referred to in Article 9 of the Act of 27 August 2009 on Public Finance;

5) a transaction carried out by a bank associating cooperative banks, if information on the transaction has been provided by an associated cooperative bank; and
6) a transfer of ownership to secure assets, effected for the term of an ownership transfer agreement with the obliged institution.

The subject to the requirements are most of the obliged entities enlisted in question 3.1 above (excluding conducting exchange office, tax advisors, notaries, attorney, legal counsels).

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

The obliged institutions are required to apply financial security measures for establishing business relationships and occasional transactions. Financial security measures include: identifying the customer and verifying the customer's identity; identifying the beneficial owner and taking reasonable measures to verify that person's identity, and determine the ownership and control structure in the case of a customer being a legal person or an organisational unit without legal personality; assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship and conducting ongoing monitoring of the business relationships of the customer.

The risk assessment depends on the type of customer, the geographic area, the purpose of the account, the type of products, services, and manners of their distribution, the level of assets to be deposited by the customer or the value of the transactions undertaken and the purpose, regularity or duration of the business relationship.

Firstly, obliged institutions are obliged to apply increased financial security measures when the client is referred to as having a higher risk of money laundering and terrorist financing. An example of situations that indicate a higher risk is: the customer is a legal person or an organisational unit without legal personality whose activity has the purpose of holding personal assets; and/or the business relationship is established in unusual circumstances.

Additionally, if the client is classified as a low-risk entity, the obliged institution may then apply simplified financial security measures.

Institutions obliged during a business relationship with a politically exposed person apply additional measures such as obtaining senior management approval for establishing or continuing a business relationship with a politically exposed person, taking adequate measures to establish the source of wealth and the source of assets available to a given customer under the business relationship or a transaction and increased conduct of ongoing monitoring of the business relationships of the customer.

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

The Polish Act prohibits making or continuing correspondence with shell banks to financial institutions referred to in Article 2 para. 1 points 1–5, 7–11, 24 and 25 of the Polish Act, i.e. banks and other financial institutions.

**3.9 What is the criteria for reporting suspicious activity?**

An example of such activity can be:

1) strange customer behaviour (the client shows signs of nervousness and/or fear);
2) the client is observed or accompanied by suspects;
3) issuing orders by third parties;
4) handing cash to the customer at the cash register window by third parties;
5) frequent transactions – several transactions of the same type in one day;
6) an extraordinary way of transporting money;
7) money is deposited in a rare currency; and
8) an irrational choice by the client of the branch of the obligated institution located far from their place of residence or seat.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

Yes, there is a National Court Register in Poland, where data about legal entities and their management and ownership is public. In addition, on 13 October 2019 the Central Register of Beneficial Owners started to operate. This register contains information such as identification data of the beneficial owners and a member of a body or a partner authorised to represent the companies and partnerships. The partnerships were obliged to notify their ultimate beneficial owner ("UBO") to the Central Register of Beneficial Owners ("CRBO") until 13 April 2020.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Such information can be found on transfer orders but it is not required by law.

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

The Act of 30 August 2019 amending the Act of Companies Code, entering into force on 1 January 2021, introduces changes in this field, i.e. dematerialisation of shares in non-public companies, setting up special registers containing information on who, in what number and in which companies owns shares.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

No, the Polish Act is not applied to entities other than those specified in question 3.1.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

No such requirements exist.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

In 2019 there have been a few amendments to the Polish legislation, among which the biggest change concerned Article 154 of the Polish Act, which specifies who can be punished for violation of its obligations. Once the amendment enters into force, penalties of up to PLN 1 million may be imposed on senior management and an employee in a managerial position responsible for compliance with the Polish Act.

Member States (including Poland) still need to implement in their national laws the provisions of the 5th and 6th AML Directives. As the timeframe for implementation of the 5th AML Directive is 10 January 2020, the Polish Ministry of Finance has already announced its plans to publish a draft act amending the current Polish Act. Some of the provisions of the 5th AML Directive have been already implemented (such as the register of beneficiaries and the extension of the catalogue of obliged institutions to entities operating in the field of virtual currencies); however, there are still some details that need to be implemented (the limitation of the possibility of using anonymous pre-paid cards and the obligation to implement specific precautions in cooperation with entities from countries outside the European Union).

On the horizon there is also an obligation to implement the provisions of the 6th AML Directive (until 3 December 2020). The Directive lists 22 specific source offences related to money laundering which should be criminalised in all EU countries (i.e. environmental crime, cybercrime and direct and indirect tax crimes).

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

No, there are not.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

In 2013, the Council of Europe (Moneyval) carried out an evaluation of the Polish system of anti-money laundering and financing of terrorism. There have also been two Compliance Enhancing Procedures in this field – the second and last compliance report was published on 3 July 2018. On 24–25 September 2019, Moneyval commenced its fifth-round mutual evaluation of Poland, which started with training authorities and representatives from the private sector on the evaluation process. The training is conducted one year in advance of the onsite visit to familiarise all national stakeholders involved in the evaluation with the underlying standards and methodology of the FATF.

**4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?**

The Polish Act is publicly available in English. The English language version is available at the Ministry of Finance website: https://www.gov.pl/documents/3297389/3574417/ustawa_tekst_EN__15062018-f__16072018.pdf.

## Acknowledgment

The authors would like to thank Miłosz Salagan for his contribution to the writing of this chapter. Mr. Salagan graduated from the Faculty of Law and Administration at the University of Warsaw. In his work he draws on his experience in private legal advisory and in public administration. Initially, he worked with the Legal Department of one of the Ministries, and then became employed with the Polish Financial Supervision Authority (Investment Funds and FinTech Departments). Mr. Salagan specialises in public regulation and supervision of financial institutions.

**Wojciech Kapica** is a partner at the firm. An expert on financial sector regulations, compliance and financial institutions ethics, he co-manages the financial markets law practice at the firm. Mr. Kapica holds a law degree from the University of Warsaw and completed a post-graduate programme in management and finance at the Warsaw School of Economics. He is an Approved Compliance Officer (ACO) certified by the Compliance Institute and Viadrina Compliance Centre. Mr. Kapica is a specialist in banking capital law, insurance law, supervisory policy and corporate governance specific to regulated businesses. He has published dozens of papers and designed training curricula on banking, insurance and anti-money laundering (AML) regulations and is the editor and co-author of a book on AML.

**SMM Legal Maciak Mataczyński**
ul. Mokotowska 33/35
00-560 Warszawa
Poland

Tel: +48 600 977 567
Email: wojciech.kapica@smmlegal.pl
URL: www.smmlegal.pl

**Magdalena Jaczewska** is an associate at the firm. Ms. Jaczewska holds a double degree in Law, awarded by the Faculty of Law and Administration of the University of Warsaw, and in Finance and Accounting, earned at the Warsaw School of Economics. She is a British Law Centre graduate, a programme in British and European law organised by the Juris Angliae Scientia in cooperation with the University of Cambridge. Currently, she is working on her Ph.D. dissertation concerning European AML regulations at the University of Warsaw.
Ms. Jaczewska started building her professional experience while still in college, working in prestigious international law firms where she specialised in handling civil disputes regarding loans in foreign currencies. She was also involved in (public and private) issues of debt securities, as well as due diligence audits in the fields of finance and insurance law.

**SMM Legal Maciak Mataczyński**
ul. Mokotowska 33/35
00-560 Warszawa
Poland

Tel: +48 609 293 069
Email: magdalena.jaczewska@smmlegal.pl
URL: www.smmlegal.pl

SMM Legal Maciak Mataczyński is one of the biggest law firms in Poland, employing 90 experienced lawyers. We provide legal services to over 200 companies, including 30 corporations quoted at Warsaw Stock Exchange. In our work, we skilfully combine academic knowledge and practical business experience. Year after year, we are featured in *The Legal 500* international ranking.
Strong expertise and extensive experience of our team members, including qualified lawyers previously working with regulatory authorities, put our Firm in a unique position to offer top-quality legal and regulatory advisory to financial institutions. We offer services in the area of regulatory and legal advisory to banks, brokerage houses, clearing institutions and other financial businesses based on our experience in a variety of fields. Our lawyers are the authors of a practical guide to the new Act on preventing money laundering and financing of terrorism, which is the first such guide on the market.

**www.smmlegal.pl**

# Portugal



Tiago Geraldo


Frederico Machado Simões

Morais Leitão, Galvão Teles, Soares da Silva & Associados


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

The Public Prosecutor prosecutes at national level and is assisted by police agencies. The Central Bureau of Investigation and Prosecution and the Judiciary Police's Financial Intelligence Unit have competency for anti-money laundering and combatting the financing of terrorism operations.

### 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. Predicate offences include, e.g., tax evasion, bribery and corruption, influence peddling, trafficking (arms, organs, drugs) and any crime punishable with a minimum sentence above six months' imprisonment or 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. Portuguese criminal law applies provided that any stage of the money-laundering process relates in any way to the Portuguese territory (e.g. funds transferred to Portuguese banks).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The public prosecutor – and the police agencies – have full competency regarding money-laundering criminal offences. However, the Bank of Portugal, the Portuguese Securities Exchange Commission, the Registry and Notary Office, the Real Estate and Construction Authority and the Tax Authority, among others, are also responsible for investigating regulatory infractions related to money-laundering offences.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

There is both corporate and natural person criminal liability for money-laundering criminal offences and related regulatory offences.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The imprisonment penalty may range up to a maximum of 12 years, although this is always limited to the maximum sentence applicable to the predicate offence, if lower. In case of legal entities, the imprisonment sentence is converted into a fine penalty. One day of prison corresponds to a 10-day fine, and each day of fine corresponds to an amount of between €100 and €10,000, which the court shall set depending on the economic and financial situation of the convicted entity and its expenses with employees.

### 1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is 15 years (without prejudice of potential causes of interruption or suspension, which may impact the calculation of the maximum time period).

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes, currently the enforcement applies only at the national level.

### 1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The Judiciary Police's Asset Recovery Bureau is responsible for the identification, tracing and seizure of the proceeds of crime. 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?**

All criminal actions are resolved through judicial proceedings. The records of the proceedings become public, at the latest, during 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. In other businesses, the responsible authorities are professional associations and other government agencies and authorities with supervisory powers within the relevant business sector.

**2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?**

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. In other businesses, the responsible authorities are professional associations and other government agencies and authorities with supervisory powers within the relevant business sector.

**2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?**

Yes, some professional associations are responsible for anti-money laundering compliance and enforcement against their members, including the legal requirements.

**2.4 Are there requirements only at national level?**

No, there are also requirements at the European Union level. Law 83/2017 is a national transposition measure of Directive (EU) 2015/849 (4th AML Directive).

**2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?**

Please see question 2.1 above: the agencies/authorities responsible for compliance and enforcement of anti-money laundering requirements are the same. There are sector-specific regulations that complement Law 83/2017, such as Notice 2/2018, issued by the Bank of Portugal to the banking sector.

**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") within the Judiciary Police. The FIU is responsible for preparing and updating statistical data related to suspicious transactions that have been reported and their results, and data related to transnational information requests that have been sent, received or refused by the FIU.

**2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?**

Concerning regulatory offences, under Law 83/2017, the statute of limitations is five years, with possible suspension and interruption of this period under certain circumstances.

**2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?**

Failure to comply with the regulatory/administrative anti-money laundering requirements may entail penalties of up to €5,000,000, depending on the nature of the entity, which may be aggravated up to double of the economic benefit obtained with the infraction or up to 10% of the annual turnover in certain cases.

Penalty provisions include: (i) illegitimate disclosure of information, communications, analyses or other elements, to clients or third parties; (ii) disclosure or improper favouring of identity discovery of those who provided information, documents or elements concerning suspicious transactions; and (iii) non-compliance with orders or legitimate instructions from sectorial authorities, 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?**

In addition to monetary fines, regulatory offences may entail additional sanctions such as: (i) losing for the State the object of the offence and the economic benefit derived from it; (ii) closing of the establishment where the agent develops the activity or job related to the offence, for a period of up to two years; (iii) prohibition of professional activity or job related to the offence, for a period of 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 of up to three years; and (v) publication of the definitive conviction.

**2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?**

There are both administrative and criminal penalties in case of violations of anti-money laundering obligations. Besides the crime of money laundering itself, crimes related to violations of anti-money laundering obligations include (i) illegitimate disclosure of information, (ii) disclosure and improper favouring of identity discovery, and (iii) non-compliance with lawful orders or instructions from the competent agencies/authorities.

**2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?**

The process for assessment and collection of sanctions is carried out by several different government agencies and authorities, listed above (see question 2.1 above), depending on the type of institution or obliged entity. The process has an administrative procedural stage where the defendants may defend themselves after a formal indictment is issued. If the competent authority decides to impose a sanction on an individual or legal entity, the latter may appeal to a judicial court.

Not all administrative resolutions become public, although the secrecy regime, applicable to the proceedings in their administrative stage, elapses with the final decision.

Several financial institutions have challenged penalty assessments in judicial and regulatory proceedings.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

The financial institutions subject to anti-money laundering requirements are: (i) banks, including credit, payment and electronic money institutions; (ii) investment firms and other financial companies; (iii) self-managed securities and real estate investment companies; (iv) 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; (v) securitisation companies; (vi) companies which commercialise contracts relating to the investment in tangible assets to the public; (vii) investment consultants; (viii) pension fund management companies; and (ix) companies and insurance intermediaries with activity in life insurance. These requirements also apply to: branches located in Portuguese territory of any of the previous entities headquartered abroad, as well as to any offshore financial centres; to payment institutions headquartered in another EU Member State, when operating in Portuguese territory through agents; or any electronic money institutions headquartered in another EU Member State, when operating in Portuguese territory through agents or distributors. Any of the previous entities operating in Portugal under the free provision of services may have to render information to the relevant sector authority. The agents and distributors, whether natural or legal persons, are also subject to anti-money laundering requirements.

The following professional activities are also subject to anti-money laundering requirements: (i) providers of gambling, lottery or betting services, whether in an establishment or online; (ii) non-financial real estate entities; (iii) auditors, external accountants and tax advisors, whether as natural or legal persons; (iv) lawyers, solicitors, notaries and other independent legal professionals; (v) trust or company service providers in certain activities; (vi) other professionals who intervene in operations of selling and buying rights over professional sports players; (vii) economic operators exercising auction or lending activities; (viii) economic operators importing or exporting rough diamonds; (ix) entities authorised to exercise the activity of transportation, custody, handling and distribution of funds and values; and (x) other entities/persons trading in goods where payment is made in cash.

Some requirements are also applicable to crowdfunding platforms, of the loan and capital type, and managing entities of crowdfunding platforms, in the categories of donation and reward and non-profit organisations.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

Crypto exchanges are not subject to anti-money laundering requirements for the purpose of Law 83/2017. However, the EU Directive 2018/843, from May 30th 2018, stipulates that virtual currency exchanges and custodian wallet services shall be considered as obliged entities, forcing Portugal to amend said Law before January 10th 2020, extending the obligations provided therein to those service providers. Furthermore, the Bank of Portugal issued the circular letter 11/2015/DPG, endorsing credit, payment and electronic money institutions to refrain from buying, owning or selling virtual currency, to prevent a variety of risks, including money laundering. The Bank of Portugal also restated that financial institutions must assess the transfers of funds with the origin and destination on virtual currency trading platforms, in the light of prevention of money laundering and terrorism financing requirements.

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

Financial institutions must maintain an independent, permanent and effective "function of compliance" to monitor and enforce internal control procedures regarding anti-money laundering and other risks. The Bank of Portugal defines several requirements for this "function".

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

There are no thresholds for reporting transactions suspected of money laundering. All suspicious transactions ought to be reported, regardless of the amounts involved.

The reporting of suspicious transactions is directed at the Central Bureau of Investigation and Prosecution and the Financial Information Unit and must be performed as soon as the suspicion arises and whether the operation has been merely proposed or attempted, if it is under course or it has already been concluded. The report must, at least, include: (i) the identification of the natural or legal persons involved, as well as any known information on their activity; (ii) the specific procedures carried out; (iii) the characterising and descriptive elements of the relevant or envisaged operation; (iv) the specific suspicious factors identified; and (v) a copy of all supporting documentation obtained through due diligence.

All entities subject to anti-money laundering requirements must keep records for a period of seven years, from the moment the client was identified, or, in case of a business relationship, from the moment it was terminated, of all documents and data obtained from clients, as well as all documents pertaining to the client's files and accounts, and all documentation produced in compliance with legal requirements, such as the documents gathered and sent to the relevant authorities to comply with reporting duties.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

According to Ordinance 310/2018, from December 4th 2018, all entities subject to anti-money laundering requirements must communicate to the Central Bureau of Investigation and Prosecution and to the FIU cash transactions of €50,000 or more, but also transactions of those values by cheques or any other paper document drawn on the payment service provider. In addition, fund transfers of €50,000 or more to or from risky jurisdictions, early repayment of funds and insurance policies of €50,000 or more and operations or transactions of gambling services providers must be communicated as well. A list of red flags can be found at http://portalbcft.pt/.

**3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?**

The anti-money laundering requirements are applicable to all transactions, regardless of whether they are national or cross-border operations. Within the EU, there is a level playing field regarding applicable requirements and authority control and information sharing. If the transaction is carried out in the context of a correspondent relationship or with a high-risk third party, there are no specific requirements for reporting, but the operation's risk profile is increased, which warrants enhanced due diligence measures.

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

Entities subject to anti-money laundering requirements must comply with customer identification and due diligence requirements whenever they establish a business relationship or when carrying out an occasional transaction that: (i) amounts to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; or (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council, exceeding €1,000.

For providers of gambling, lottery or betting services, the threshold corresponds to transactions amounting to €2,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

Such requirements apply whenever there is a suspicion of money-laundering practices, regardless of any derogation, exemption or threshold or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Customer identification and due diligence require obtaining identification elements, the activity exercised, documents to verify such elements and information regarding the purpose and nature of the intended business relationship. When the 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 constant monitoring of the business relationships to ensure that the operations carried out in their course are consistent with the knowledge the entity has of the activities and risk profile of the client, and the origin and destination of the movement of funds.

Due diligence requirements are enhanced whenever there is a transaction involving high-risk third countries, non-face-to-face business relationships or transactions, politically exposed persons or other high public and political offices, life insurance policies or cross-border correspondent relationships with third-country institutions, as provided in Regulation 2/2018 of the Bank of Portugal.

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

Law 83/2017 prohibits financial entities from establishing or maintaining correspondent relationships with shell banks or to establish or maintain correspondent relationships with financial institutions which allow their accounts to be used by shell banks.

**3.9 What is the criteria for reporting suspicious activity?**

If an entity knows, suspects or has enough grounds to believe that certain funds or other assets, regardless of amount, originated from criminal activity or are related to terrorism financing, that entity must report the activity.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

There is a public corporate registry that can be accessed through a code for each individual company. The legislation regarding a central register for beneficial owners entered into force on November 19th 2017. The purpose of this register is to provide,

through different levels of access, information regarding the ultimate beneficial ownership of legal entities, amongst others, to financial institutions and other entities which are subject to anti-money laundering requirements, and to customer due diligence responsibilities.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Accurate information on originators and beneficiaries will depend on the client's risk profile and the features of the operation.

In the specific case of funds transfer not associated with an account, the financial institution of the originator or the beneficiary must collect a certain amount of information, depending on the type of the entity, regarding the originator or beneficiary's identification, if the transfer amounts to €15,000 or more (according to Regulation 5/2013 from the Bank of Portugal).

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

No, not since 2017.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

Yes, there are certain requirements that are specific to providers of gambling, lottery or betting services, regarding, for example, the form of prize payment. Specific requirements also apply to legal professionals, although there is a derogation of the reporting duty whenever the services provided for the client are in the context of a judicial process.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

Under Portuguese jurisdiction, trusts can only be registered in the free trade zone of Madeira, with applicable anti-money laundering requirements such as the gathering of information on their beneficial ownership, to be declared to the Central Register of Beneficial Owners.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

Aside from Regulation 2/2018, from September 11th 2018 of the Bank of Portugal, there are other sectorial authorities which have already proposed and published additional measures, such as the Economic and Food Safety Authority and the Real Estate and Construction Authority. Other sectorial authorities are preparing additional regulatory instruments, such as the Portuguese Securities Exchange Commission.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

In the last FATF evaluation (December 2017), Portugal was considered to have a sound and effective legal framework in place to combat money laundering. According to that evaluation, Portugal was deemed Compliant for 12 and Largely Compliant for 22 of the FATF 40 Recommendations. The areas of non-profit organisations, correspondent banking, wire transfer, customer due diligence of designated non-financial businesses and professions, transparency and beneficial ownership of legal persons were deemed partially compliant.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The FATF conducted an onsite visit (March 28th–April 13th 2017) and then produced a Mutual Evaluation Report in December 2017, as mentioned above.

**4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?**

The AML/CFT Coordination Commission, established in 2015, is responsible for the overall policy coordination and implementation of AML, CFT and counter-proliferation financing measures. Relevant legislation and guidance can be accessed on their homepage, at the following link: http://portalbcft.pt/ (not available in English). Some sectorial authorities have internet pages in English, such as the Bank of Portugal (https://www.bportugal.pt/). The Public Prosecutor's office has a collection of criminal law-related legislation translated into English (http://gddc.ministeriopublico.pt/pagina/portuguese-legislation-english), but more often than not legislation is not translated into English.

**Tiago Geraldo** joined Morais Leitão in 2008. He is a member of the firm's litigation department.
His practice focuses on the area of criminal litigation, including regulatory offences and particularly on economics and finance.
He also collaborates within the areas of competition law, corporate law, labour law and tax law, regarding criminal or quasi-criminal issues.
Concurrently, 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, auditing, energy, telecommunications and media.
Tiago regularly participates in conferences and post-graduate courses on criminal law and criminal procedure, misdemeanour and compliance. He has published several articles on these matters.
Moreover, Tiago is a lecturer at the University of Lisbon School of Law, where he is also a member of the Center for Investigating Criminal Law and Sciences and a founder of the Criminal Law and Sciences Institute.

**Morais Leitão, Galvão Teles, Soares da Silva & Associados**
Rua Castilho, 165, 1070-050
Lisbon
Portugal

Tel: +351 210 091 783
Email: tgeraldo@mlgts.pt
URL: www.mlgts.pt

**Frederico Machado Simões** joined the firm in May 2017. He is a member of the litigation and arbitration team.
Previously, Frederico completed an internship at Liberum Advogados (January 2016).
On the academic circuit, Frederico is a researcher at the Center for Research in Criminal Law and Criminal Studies.

**Morais Leitão, Galvão Teles, Soares da Silva & Associados**
Rua Castilho, 165, 1070-050
Lisbon
Portugal

Tel: +351 210 091 750
Email: fmsimoes@mlgts.pt
URL: www.mlgts.pt

Morais Leitão 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, Morais Leitão has its head office in Lisbon and offices in Porto and Funchal (Madeira Island). To support clients' international strategies, Morais Leitão developed a network of associations with local firms in Angola, Mozambique, Macau and Hong Kong – Morais Leitão Legal Circle, which offers integrated multijurisdictional teams.

**www.mlgts.pt**

# Romania


Simona Pirtea

Mădălin Enache

Enache Pirtea & Associates


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

In Romania, all prosecution is conducted by the Public Ministry, organised in Prosecutors' Offices with the courts of law (Ordinary Courts, Tribunals, Courts of Appeal, the High Court of Cassation and Justice "HCCJ").

The Prosecutors' Offices with Tribunals have general competence to prosecute money-laundering crimes. However, any other superior Prosecutors' Office can also prosecute money laundering if, in the investigation of other crimes within their competence, they uncover such deeds committed by the same person or having a strong link to these. In addition, the specialised Prosecutors' Offices (National Anticorruption Directorate – "NAD" and the Directorate for Investigating Organized Crime and Terrorism – "DIOCT") can prosecute money laundering if the predicate crime is within their competence.

### 1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Money laundering is provided by Law no. 129/2019 ("Law 129"), art. 49, defining it as one of the following conducts:

- conversion or transfer of property, knowing that such property is derived from criminal activities, for the purpose of concealing or disguising the illicit origin of that property or of assisting any person who was involved in the criminal activity to avoid the legal consequences of his action;
- the concealment or disguise of the true nature of the origin, location, disposition, movement, ownership or rights with respect to such property, knowing that such property is derived from criminal activities; and
- the acquisition, possession or use of property, knowing that the property is derived from criminal activities.

Law 129 does not limit the range of crimes which can be considered predicates for money laundering. As a result, any offence that leads to obtaining "dirty" money or properties can be the predicate for money laundering.

Tax evasion is a recurrent predicate crime for money laundering, as there is a very wide range of criminal cases having as their object charges/accusations of tax evasion, together with money laundering. Receipt of bribes or misuse of EU funds are other common predicate crimes.

### 1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

As per art. 9 of the Criminal Code, Romanian criminal law (Law 129 included) applies to crimes committed outside Romanian territory by a Romanian citizen/legal entity if the act is also outlawed by the criminal law of the country where it was committed, or if it was committed in a location that is not subject to any jurisdiction.

As stated in the Preliminary Ruling Decision no. 16/2016 of the HCCJ, Romanian criminal law does not require a prior or simultaneous conviction for a predicate offence in order to obtain a conviction for money laundering, thus money laundering is an autonomous crime. *A fortiori*, money laundering of the proceeds of foreign crimes is punishable (especially if there is a conviction decided where the offence was committed).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Besides the Prosecutors' Offices (as presented above), investigations can be conducted at a preliminary stage by the National Office for Prevention and Control of Money Laundering ("NOPCML"), which is the Romanian FIU and leading supervisory authority regarding money laundering. As soon as it identifies indications/suspicions of money laundering (as a crime), NOPCML must immediately inform the Prosecutors' Office to launch an official investigation. NOPCML has also the competence to collect and process relevant information to facilitate the activity of the prosecutors, as per their request.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

Starting from 2006, the Romanian Criminal Law introduced criminal liability for legal entities if the crimes are committed in the performance of the object of activity of legal entities or in their interest or behalf.

This is a general provision, hence it also applies to money-laundering crimes. The corporate criminal liability does not exclude the criminal liability of the involved natural persons.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

For individuals, money laundering is punishable with three to 10

years of imprisonment. For legal entities, the main penalty is the fine, which can be set at any value from RON 18,000 (approx. EUR 3,900) to RON 1,500,000 (approx. EUR 326,000).

**1.7 What is the statute of limitations for money laundering crimes?**

For money laundering, the general statute of limitations is eight years. However, the special statute of limitations of 16 years might also apply, should criminal proceedings (including trial) be launched against the persons.

**1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?**

Romania is a national state, the reason for which there is only one authority – the Prosecutors' Office with the HCCJ – which can conduct criminal investigations. As mentioned, this is organised with central and local structures, including specialised directions (NAD and DIOCT, also with local structures) and a special Section for Investigating Justice Crimes ("SIJC") – crimes committed by judges and 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?**

Asset forfeiture can be ordered by any prosecutor and court of law against the goods of a defendant, while confiscation can only be ordered by a court of law, along with a criminal conviction.

The object of the forfeiture/confiscation can be any money, goods or assets which were produced by the criminal activity and were: used in any way or intended to be used in the activity; used to ensure the perpetrator's escape; given to reward the perpetrator; acquired by perpetrating the offence; or if their possession is prohibited by the law. If the goods were transferred to third parties of good faith, cannot be found or they have been alienated, the authorities can confiscate the equivalent of their value or the price. Without a criminal conviction, confiscation can be instituted on the property of third parties only if it is a direct or indirect product of the crime.

Furthermore, in 2015 it was established, under the authority of the Ministry of Justice and the National Agency for the Management of Seized Assets ("NAMSA"), in order to facilitate asset recovery by combining the support of the criminal prosecution bodies with the attributes of international cooperation, management of seized assets and social reuse of confiscated assets.

**1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?**

There have been several criminal investigations into bank executives and officers for collusion to money laundering, yet there exists no public record of any conviction. In late February 2020, the Romanian National Bank ("RNB") announced that 16–17 national banks (or branches) are suspected of being involved in suspicious transactions related to possible money-laundering operations, but no public confirmation in this regard exists from the prosecutors.

**1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?**

If the individual or the legal entity is considered guilty, the criminal actions can be resolved only in front of a Court of law. No settlement can be concluded only by the prosecutor/other authority and the perpetrator.

However, Romania introduced in 2014 the possibility for defendants and prosecutors to conclude a Deferred Prosecution Agreement ("DPA"), by which the defendant admits guilt and recognises the accusations in exchange for a diminished penalty (usually a prison conviction with a suspended execution), but a Court must still verify the lawfulness and the terms of the DPA and admit it.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

**2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.**

Only Parliament can impose legislation (as with Law 129 for AML). Financial institutions are also regulated by specific bodies, which can complete or detail, through general applicability Orders, these norms. The authorities invested with the supervision of compliance with the legal requirements are:

a) the prudential supervision authorities (such as the RNB or Financial Supervisory Authority ("FSA")), for the entities that are subject to their supervision, including the branches of foreign legal persons that are subject to a similar supervision in their country of origin;
b) the National Anti-Fraud Agency, with tax and financial control attributions; and
c) the NOPCML, as provided by Law 129.

The legal requirements consist of the following main obligations: KYC rules; obtaining information about the real beneficiaries; designation of AML officer; reporting of suspicious transactions to the NOPCML; freezing of operations pending NOPCML clearance; safeguarding all relevant evidence of suspicious transactions; and not informing the clients about any AML investigations.

**2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?**

No, the AML requirements are imposed only by the law. Nevertheless, self-regulatory organisations or professional associations can elaborate guides and recommendations for compliance with AML requirements. For example, *The Guide for the best practices of reporting suspect transactions which might involve money laundering or terrorism financing* was released by the Chamber of Financial Auditors of Romania in 2016.

**2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?**

The leading structures of the independent legal professions (e.g.

auditors, tax or accounting consultants, lawyers, public notaries) must designate one or several AML officers as per Law 129. These persons must establish adequate policies and procedures (KYC, real beneficiaries reporting, AML reporting, secondary and operative recordkeeping, internal control, training, etc.) in order to prevent and stop any money-laundering and terrorism-financing operations by its members. Regardless of the cooperation existing on AML between these structures and the NOPCML, they are not directly responsible for non-compliance of their members.

**2.4 Are there requirements only at national level?**

Yes, with general applicability.

**2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?**

Please see question 2.1 for the authorities mentioned, based on the provisions of Law 129 and derivative legislation.

**2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?**

The NOPCML, as presented above, is Romania's FIU, with duties of preventing, sanctioning or reporting money-laundering activities. The NOPCML receives/requests, analyses and processes information originating from institutions/entities having AML obligations.

**2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?**

From the moment when the violation act ends, the authorities have six months to apply a sanction/contravention, which must be communicated to the offender by a further maximum of two months. If the deed is considered a crime, the general (and possibly special) statute of limitations applies (please see question 1.7 above). The NOPCML is the authority with competences related to discovering and sanctioning the contraventions. Moreover, the NOPCML is responsible for transmitting to the criminal investigation bodies any suspicions about possible money-laundering crimes.

**2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?**

Breaching the provisions of Law 129 may constitute a contravention, sanctioned with a fine of up to RON 150,000 (approx. EUR 31,000), or, in special cases in which the breach is serious, repeated and/or systemic, legal entities can be fined by up to RON 5,000,000 (approx. EUR 1,040,000).

The following misconduct may be sanctioned with the highest fine: failure to transmit requested information to NOPCML within 15 days (or 48 hours, in urgent matters); failure to comply with the adequate KYC measures or with the obligation to designate an AML officer; (for credit and financial institutions) opening/operating an anonymous account or an account which does not permit a proper identification of the client; and (for the institutions and the authorities with supervision duties) failure to accomplish their duties.

**2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?**

The individuals cannot be the subject of other types of sanctions in an administrative (and not criminal) procedure.

For legal entities, Law 129 establishes the following accessory sanctions for non-criminal violations: confiscation of the goods that have been used in, destined to be used in or obtained from committing the violation; suspension/annulment of the authorisation to engage in the activity; withdrawal of the licence for certain operations or for foreign trade activities; freezing of the bank account; suspension of the activity of the entity; and shutting down the entity's unit. Moreover, for entities targeted by prudential control, the supervision authorities (the RNB or FSA) can impose specific sanctions for their type of activity.

**2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?**

The penalties can be administrative, civil, or disciplinary. In addition to this, criminal sanctions can be applied for violating the interdiction to transmit information regarding the money laundering or terrorism financing and in case of any leaks of information to the client about an ongoing NOPCML investigation, both to the financial institutions and/or their representatives. Any sanction results in the obligation of the entity to comply with the legal provisions, otherwise they can be sanctioned again with an even higher penalty. All types of penalties can be applied cumulatively to the company and its directors, officers or employees, if they have a concurring personal fault. Moreover, as an auxiliary penalty, the individuals can be banned from the exercise of the profession or occupation they have used for committing the crime.

**2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?**

a) No, the general practice is that the resolutions of penalty actions are not public.
b) Yes, it is a common practice to challenge any penalty that is imposed by the authorities.

The administrative sanctions can be applied by NOPCML or by the prudential supervision authorities (for the entities supervised by them) and they can be appealed in Court, like any other administrative sanction in the Romanian legal system.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

According to art. 5 of Law 129, the following entities are scrutinised:

a) credit institutions and branches in Romania of the foreign credit institutions;
b) financial institutions, as well as branches in Romania of the foreign financial institutions;
c) private pension funds administrators, on their own behalf and for the private pension funds they manage, marketing agents authorised for the system of private pensions;
d) casinos;
e) auditors and natural and legal persons providing tax and accounting consultancy;
f) public notaries, lawyers, judicial executors and other persons exercising independent legal professions, when they assist in planning or executing transactions for their customers concerning the purchase or sale of immovable assets, shares or interests or trade funds, managing of financial instruments, movable assets or other assets of customers, operations or transactions which imply an amount of money or a transfer of property, opening or management of bank, savings, accounts or of financial instruments, organisation of contributions necessary for the creation, operation, or management of a company; creation, operation, or management of companies, undertakings for collective investments in transferable securities, other trust activities or when they act on behalf or in the name of their clients in any financial or real estate transactions;
g) service providers for companies or other entities, other than those mentioned in para. e) or f);
h) persons with duties in the privatisation process;
i) real estate agents; and
j) other natural or legal persons that trade goods and/or services, provided that the operations are based on cash transactions, in RON or foreign currency, whose minimum value represents the equivalent in RON of EUR 10,000, indifferent if the transaction is performed through one or several linked operations.

The credit institutions and the financial institutions must have internal rules and procedures for KYC and swift collaboration with NOPCML, on demand.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

Law 129 introduced, for the first time in the Romanian legislation, special obligations for the cryptocurrency industry. In this respect, agents and distributors of cryptocurrencies and payments' institutions (including foreign) must respect and ensure that their agents and distributors respect and comply with the legal provisions regarding AML.

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

All entities subject to Law 129 must adopt adequate AML measures and apply risk-based standard/simplified/additional customer due diligence measures, in which to identify, where applicable, the real beneficiary. The financial institutions must also apply AML measures of customer identification to foreign branches and subsidiaries.

In addition, reporting entities must also appoint one or multiple officers to handle the relation with NOPCML; these persons must have specific responsibilities and NOPCML should be informed about their names and the nature and limits of their specific duties.

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

Reporting entities must implement secondary or operative recordkeeping policies, designed for internal control, risk assessment and management, so as to obstruct and prevent operations suspected of money laundering. When client identification is required, these entities have the obligation to keep copies of identity documents for a period of five years, from the date when the relationship with the client is terminated. Moreover, a track record of all the measures taken for the identification of the real beneficiaries must also be kept.

Reports to NOPCML must be filed within three working days from the internal or external transaction(s) with cash, in RON or foreign currency, whose minimum threshold represents the equivalent in RON of EUR 10,000, or through bank accounts whose minimum threshold represents the equivalent in RON of EUR 15,000, irrespective of whether the transaction is performed in only one operation or in several operations that seem interconnected.

For money transfer services, the minimum threshold is EUR 2,000.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

No, there are none.

**3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?**

There are no specific obligations – the general rules of reporting apply.

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

Law 129 stipulates three possibilities to customer-related obligations (especially KYC rules), chosen on a risk-based approach: standard; simplified; or supplementary.

The standard provisions apply: whenever a business relationship is initiated/a new client is involved; for an occasional transaction of a minimum of EUR 15,000, regardless of whether it is constituted from one or more operations which are linked; for a transfer of funds of a minimum of EUR 1,000 (as defined in Regulation (EU) 2015/847); and for the occasional transactions of a minimum of EUR 10,000 performed by the merchants, in their professional activity, regardless of whether they are constituted from one or more operations which are linked.

Casinos must apply standard provisions to clients which collect winnings, buy or exchange chips or when transactions are made with a minimum equivalent of EUR 2,000.

The simplified provisions can be applied when the clients are graded as low risk. The low-risk grade can result from the global evaluation of the risk factors with regards to the client (public entities with reporting obligations, public enterprises, clients from low-risk geographic areas), to the products, services, transactions or distribution channels (life insurance, social securities, products with low money-laundering risks) or to the geographic area (Member States, AML-efficient countries, etc.).

The supplementary provisions apply when there is an increased risk of money laundering due to: non-AML compliant countries involved in transactions; correspondent relationships with credit or financial institutions from another Member State; the correspondent relationship with non-EU/non-EEA credit institutions; or the other party or the real beneficiary is a politically exposed person.

The standard measures are:

a) identifying the client and verifying his identity in trustworthy sources, including documents;
b) identifying the real beneficiary and risk-based verification of his identity, as to guarantee sufficient knowledge over the entity's ownership and control structure;
c) obtaining information about the purpose and the nature of the business; and
d) continuously monitoring the business relationship, including analysing transactions, to ensure that they correlate with the information about the client, his risk-based/activity profile and the source of funds. The documents, data and information should always be updated.

The entities that apply AML measures are not obliged to apply the provisions for clients with cryptocurrencies, if all the following conditions are met:

a) the payment instrument is not rechargeable or has a maximum limit of EUR 150 for monthly payment transactions, which can be used only in the respective Member State;
b) the maximum amount deposited electronically does not exceed EUR 150;
c) the payment instrument is used exclusively to purchase goods or services;
d) the payment instrument cannot be financed with anonymous cryptocurrencies; and
e) the issuer carries out sufficient monitoring of the transactions or the business relationship to allow the detection of unusual or suspicious transactions.

### 3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Credit institutions are prohibited to enter into a banking relationship with a shell bank or with a credit institution that is known to allow its accounts to be used by a shell bank. In case there is an ongoing relationship, the credit institution must stop it immediately. All credit institutions are subject to this prohibition.

### 3.9 What is the criteria for reporting suspicious activity?

Law 129 defines suspicious transactions as operations apparently not having economical/legal character or having (or being suspected of having) an unusual nature in relation to the activities of a client of one of the reporting entities. All suspicious transactions must be reported to the National Office for Prevention and Control of Money Laundering ("ONPCSB") as soon as possible, and the ONPCSB must confirm receipt of the report. An additional obligation for the entity is to refrain from the operation of a connected transaction with the suspected transaction for 24 hours, the period at the end of which the transaction can be operated unless the ONPCSB orders the suspension of the transaction for 48 hours. The Prosecutors' Office with the HCCJ can order the extension of the term with an additional 72 hours for further investigations related to the suspicious transaction.

### 3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

The Romanian Government, mainly through the National Trade Registry Office, keeps detailed information regarding a company which any interested person can request access to (e.g. ownership structure, management, funding, financial records, etc.).

### 3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

When sending money from an associated account, the payment order must include the full names and bank accounts of the originators and the beneficiary. Additional information (the fiscal or personal identification number) must be included if the beneficiary of the payment order is the National Treasury.

### 3.12 Is ownership of legal entities in the form of bearer shares permitted?

Under the provisions of Law no. 31/1990, a joint-stock company has the liberty to decide whether the shares are nominative or bearer. Although bearer shares are legal, their existence in a company's structure can signal a "red flag" for the potential business partners and they might not be willing to engage in a business relationship for this reason. In addition to this, numerous auctions in the public sector allow only the participation of companies with nominative shares.

### 3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

No, the general rules of reporting apply.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

There are none that are applicable.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

Law 129 is the transposition of the 4th AML Directive – (EU) 2015/849.

The 5th AML Directive – (EU) 2018/843 has yet to be implemented (though due January 10th, 2020), the reason for which Romania has been officially notified (February) by the European Commission of impending infringement procedures (along with seven other EU states).

The 6th AML Directive (EU) 2018/1673, with an implementation deadline of December 3rd, 2020, is also being currently analysed for transposition in Law 129 (possibly along with the 5th Directive).

**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 the entering into force of Law 129, Romania is fully compliant with the recommendations of the FATF.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The last review of Romanian AML legislation was conducted by MONEYVAL in 2019 (previously in 2008).

Furthermore, in 2016 Romania was deemed a Jurisdiction of Concern by the US Department of State 2016 International Narcotics Control Strategy Report ("INCSR").

In addition, Romania is still under scrutiny of the EU through the Mechanism for Cooperation and Verification ("MCV") for the Justice System; certain recommendations are being made to strengthen the fight against corruption, including better capabilities of recovering the proceeds of crime and avoiding benefits from money laundering in relation to white-collar criminality.

**4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?**

The NOPCML website contains the main useful documents in this respect: http://www.onpcsb.ro/english-documents-on-pcsb/relevant-legislation. However, Law 129 is yet to have a publicly available English translation.

**Simona Pirtea**'s activity as a lawyer can be best described by the attributes of professionalism accompanied by strategic thinking and absolute dedication. She is a valued business law practitioner, with an intensive professional activity in the legal and the intelligence fields, having proven her strong technical knowledge and consistent business-oriented approach throughout a wide array of complex cases dealing with important multinational companies or working with governmental and European institutions in matters regarding national security, economic strategies, strategic planning and risk management.

Simona is recognised for her straight-forward and innovative legal approach, as well as for her business-integrated advice. Based on her extensive experience in criminal law and risk management and by using her knowledge and know-how obtained in this field, she has forwarded her practice conducting several major projects in compliance and regulatory. Due to her very professional expert opinion and legal advice in complex and sensitive corporate matters, Simona has become a reputed counsellor for companies confronted with internal disorders or mismanagement situations.

Simona is also notable for being a lecturer with the Superior Institute of Law and Economics in Barcelona, Spain and for having won numerous awards for her business-oriented approach as a business and criminal lawyer.

**Enache Pirtea & Associates**
32 Pictor Ion Negulici Street
1st District, Bucharest
Romania

Tel: +40 740 137 358
Email: simona@enachepirtea.ro
URL: www.enachepirtea.ro

**Mădălin Enache** has practised extensively and quasi-exclusively in high-level White-Collar and Business Crime cases since 2006, acquiring first-class professional expertise in some of the most difficult and media-scrutinised criminal investigations and trials, being known in the field as one of the highest-skilled practitioners, building a solid reputation as a leading criminal law attorney; he is acknowledged and recognised by clients and global legal publications (*Chambers Europe*, *The Legal 500*, etc.).

Mădălin has counselled, assisted and represented renowned international and Romanian corporate clients, key figure businessmen and executives, and high-profile politicians involved in a wide range of cases in front of the criminal investigation authorities or courts of law, at the highest level of jurisdictions, with a focus on mainly corruption cases, financial and fiscal frauds, embezzlements of public/EU funds, money laundering, abuse of office, etc.

Due to his practical and business-focused approach, Mădălin is a valued lecturer on criminal law topics, having also published several specialised articles in national and international publications, on different relevant topics in the criminal domain, especially in the areas of anti-bribery, money laundering and business crimes.

**Enache Pirtea & Associates**
32 Pictor Ion Negulici Street
1st District, Bucharest
Romania

Tel: +40 723 323 541
Email: madalin@enachepirtea.ro
URL: www.enachepirtea.ro

Extraordinary professionalism applied to the requirements and needs of our clients – this is what Enache Pirtea & Associates stands for. Based on our 15 years of experience in the field of Business & White-Collar Crime, our Law Firm truly goes "the extra mile", providing clients with lawyers who think business and who give them applicable cutting-edge solutions, in order to ensure businesses move forward with ethics and integrity, while people are safe to enjoy a better future.

The Firm's focal area of activity is Criminal Law – Business & White-Collar Crime, in its two main components: business crime consultancy & counselling (business ethics & integrity); and criminal investigation & litigation. We have developed unparalleled practical skills, forged in the midst of some of the fiercest and most scrutinised top-level court battles and prosecutorial inquiries (including at the international level – SFO, SEC, DOJ), mainly working for foreign corporate clients, as well as for their executives and officers, but also acting on behalf of local companies, businessmen, public figures, politicians and officials. Be it corruption crimes or money laundering, economic criminality or abuse of office, embezzlement of EU funds or cybercrime, copyright or environmental criminal breaches, we have across-the-board experience and knowledge.

**www.enachepirtea.ro**

ENACHE PIRTEA & ASOCIAȚII
BUSINESS AT LAW

# Singapore



Lee Bik Wei


Lee May Ling

Allen & Gledhill LLP


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

The Attorney-General ("**AG**"), as the Public Prosecutor ("**PP**"), has the legal authority to prosecute money laundering ("**ML**") in Singapore.

### 1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) ("**CDSA**") criminalises the laundering of proceeds generated by drug dealing/criminal conduct:

- assisting another person in retaining, controlling or using the benefits of drug dealing/criminal conduct under an arrangement (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise) (Section 43(1)/44(1));
- concealing, converting, transferring or removing from the jurisdiction, or acquiring, possessing or using property that represents a person's own benefits of drug dealing/criminal conduct (Section 46(1)/47(1));
- concealing, converting, transferring or removing from the jurisdiction property that represents another person's benefits of drug dealing/criminal conduct (Section 46(2)/47(2));
- acquiring, possessing or using property that represents another person's benefits of drug dealing/criminal conduct (Section 46(3)/47(3)); and
- possessing or using any property that may be reasonably suspected to be benefits from drug dealing/criminal conduct, if the person fails to account satisfactorily for how the person came by the property (Section 47AA(1)).

**What must be proven**

*Physical elements*: The PP must prove that the accused carried out the relevant physical act of the said offence. Under Section 43(1)/44(1), this means that the PP must prove that (i) the accused entered into or is concerned in an arrangement, (ii) which facilitated another person in retaining, controlling or using the benefits of drug dealing/criminal conduct, and (iii) that other person is a person who engages in drug dealing/criminal conduct.

Under Sections 43, 44, 46, 47, the PP must also prove that the property was the benefits of drug dealing or criminal conduct; whereas under Section 47AA, the PP must only prove that the property would be suspected by a reasonable person of being benefits from drug dealing/criminal conduct.

*Mental/fault element*: Strict liability is imposed under Sections 46(1)/47(1).

Under Section 47AA(1), the accused must give a satisfactory explanation for how he came by the property. This section was introduced to combat ML operations involving money mules.

As for the other ML offences, the PP must prove that the accused knew or had reasonable grounds to believe that:

- (i) the arrangement would facilitate the retention, control or use of another person's benefits of drug dealing/criminal conduct, and (ii) the other person is a person who engages in drug dealing/criminal conduct or has benefitted from drug dealing/criminal conduct (Section 43(1)/44(1)); and/or
- the property represents another person's proceeds of crime.

**Predicate offences**

Predicate offences are listed in the First and Second Schedules of the CDSA, and include the conspiracy, attempt, abetment or incitement of another to commit such offences. The First Schedule identifies a "drug dealing offence" (which includes the ML offences under Sections 46 and 47). The Second Schedule identifies a "serious offence" constituting criminal conduct.

Predicate offences also include foreign drug dealing or serious offences, i.e. an offence against the law of a foreign country which would also constitute an offence listed in the First or Second Schedules of the CDSA, if the conduct had occurred in Singapore (Section 2(1) CDSA).

**Whether tax evasion is a predicate offence for money laundering**

Yes. Tax evasion under Sections 96 and 96A of the Singapore Income Tax Act (Cap. 134) and the national law of a foreign country (based on specific proscribed conduct) is a predicate offence for ML (Second Schedule and Section 2(1) CDSA).

### 1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The CDSA has extraterritorial application as it applies to properties (including money and all other forms of property) in Singapore or elsewhere (Section 3(5) CDSA), and foreign drug dealing/serious offences (see question 1.2 above).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The Commercial Affairs Department ("**CAD**"), a specialist department within the Singapore Police Force, is the principal law enforcement agency for the criminal investigation of ML offences. The Corrupt Practices Investigation Bureau or the Central Narcotics Bureau may also be involved.

The Attorney-General's Chambers is responsible for prosecuting ML offences.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

There is both corporate criminal liability and liability for natural persons.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Under Sections 43, 44, 46 and 47, the penalty is:

- for an individual, a fine not exceeding S$500,000, or imprisonment not exceeding 10 years, or both; and
- for a non-individual, a fine not exceeding the higher of S$1 million or twice the value of the benefits of drug dealing/criminal conduct in respect of which the offence was committed.

Under Section 47AA, the penalty is:

- for an individual, a fine not exceeding S$150,000, or imprisonment not exceeding three years, or both; and
- for a non-individual, a fine not exceeding S$300,000.

### 1.7 What is the statute of limitations for money laundering crimes?

There is no statute of limitations for the prosecution of ML crimes.

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes. Singapore does not have state or provincial criminal offences.

### 1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

There is no separate forfeiture/confiscation authority. Upon conviction for one or more predicate offences in the CDSA, and on the PP's application, the Court may make a confiscation order against the defendant in respect of benefits derived by him or her from drug dealing/criminal conduct if the Court is satisfied that such benefits have been so derived (Sections 4 and 5 CDSA).

A confiscation order compels the defendant to pay an amount assessed to be the value of the benefit derived by the defendant from drug dealing/criminal conduct (Section 10 CDSA). Confiscation orders operate as if they were a fine imposed by the Court. In default of payment, the defendant may be subject to imprisonment.

Material/financial gains from organised crime activity can be confiscated without the need for a criminal conviction under the Organised Crime Act 2015 (No. 26 of 2015) ("**OCA**"). A confiscation order under the OCA is not dependent on and is not affected by any criminal proceedings, even if the accused is acquitted (Section 51 OCA). Upon the PP's application, the Court will make a CO if the Court is satisfied, on a balance of probabilities, that the person has carried out an organised crime activity within the defined statutory period and has derived benefits from the organised crime activity.

"Organised crime activity" refers to any activity carried out by a person in (or outside) Singapore amounting to a serious offence specified in the Schedule to the OCA (which includes Sections 43, 44, 46 and 47 of the CDSA) and is carried out at the direction of/in furtherance of the illegal purpose of a group which the person knows or has reasonable grounds to believe is an (locally linked) organised criminal group (Section 48(1)(a)–(b) OCA).

It also includes activity amounting to an offence under Part 2 of the OCA (Section 48(1)(c) OCA). Part 2 of the OCA contains a group of provisions that criminalise being a member of an organised criminal group, instructing or facilitating the commission of an offence by such a group, and recruiting of members and expending of property to support these groups.

"Property" is defined in the same way as the CDSA (Section 2(1) OCA).

### 1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Directors, officers or employees of regulated financial institutions ("**FIs**") have been convicted in Court for ML offences. One example is Yeo Jiawei, a former wealth planner at BSI Bank Limited, who was sentenced to 54 months' imprisonment for ML and cheating in a case related to the Malaysian state fund 1Malaysia Development Berhad ("**1MDB**"). A former branch manager of Falcon Private Bank, Jens Sturzenegger, was also sentenced to 28 weeks' imprisonment and a S$128,000 fine for failing to report suspicious transactions connected to the 1MDB case.

### 1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal actions against a company, partnership or unincorporated association may be resolved through the use of a Deferred Prosecution Arrangement ("**DPA**") (Part VIIA of the Criminal Procedure Code (Cap. 65A)). The DPA is an agreement between the PP and entities facing potential prosecution for certain specified criminal offences (including the MLs offences at question 1.2). A DPA comes into force only when the High Court approves it and declares that the DPA is in the interests of justice, and its terms are fair, reasonable, and proportionate. After such approval, the PP must give public notice of the DPA and the High Court's declaration and reasoning.

It is not applicable to individuals.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

### 2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The Monetary Authority of Singapore ("**MAS**") investigates alleged breaches of anti-money laundering ("**AML**") requirements on FIs in Singapore.

Other authorities that impose AML requirements on non-financial businesses and professions ("**Designated Businesses**") include:

- the Casino Regulatory Authority of Singapore (for casinos);
- the Accounting and Corporate Regulatory Authority ("**ACRA**") (for corporate service providers, public accountants and accounting entities); and
- the Council for Estate Agents (for estate agents and salespersons).

For more details of these requirements, see section 3 below.

### 2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes. These include the Institute of Singapore Chartered Accountants (for professional accountants) and the Law Society of Singapore (for law practices and legal practitioners).

### 2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, they may have their own enforcement measures against members. For example, legal practitioners and law practices are subject to AML requirements under the Legal Profession Act (Cap. 161) (including the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015), and a breach of these rules may subject the legal practitioner to disciplinary proceedings and/or the law practice to regulatory action.

### 2.4 Are there requirements only at national level?

Yes, Singapore does not have different levels.

### 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

MAS is responsible for ensuring compliance and enforcement of AML requirements under MAS-administered laws and regulations. MAS's enforcement approach is outlined in the Enforcement Monograph, which is available on the MAS website. MAS guidelines in respect of what constitutes compliance with AML requirements are also publicly available on its website.

### 2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Suspicious Transaction Reporting Office ("**STRO**") is Singapore's FIU. The STRO is the central agency for receiving, analysing, and disseminating suspicious transaction reports ("**STR**"), Cash Transaction Reports ("**CTR**") and Physical Currency and Bearer Negotiable Instruments ("**CBNI**") Reports ("**CBNIR**").

### 2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no statute of limitations for enforcement actions.

### 2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

These vary across industries.

Under Section 27B(2) of the MAS Act (Cap. 186), a FI that fails to comply with any AML direction issued or regulation made by MAS is liable to a fine not exceeding S$1,000,000, and in the case of a continuing offence, is also subject to a further fine of S$100,000 for every day or part of a day during which the offence continues after conviction.

MAS may, at its discretion, compound any offence which is punishable with a fine only by collecting from a person reasonably suspected of having committed the offence a sum not exceeding one half of the amount of the maximum fine prescribed for that offence (Section 176(1) MAS Act). On payment of such sum, no further proceedings shall be taken against that person in respect of that offence.

### 2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

These vary across industries.

For FIs, MAS can impose non-financial sanctions such as:

- revocation or suspension of regulatory status (e.g. BSI Bank Limited and Falcon Private Bank Ltd, Singapore Branch in relation to 1MDB);
- removals of directors and officers;
- prohibition orders ("**PO**") barring persons from conducting regulatory activities or from taking part in management of the FI (e.g. MAS has issued POs against numerous individuals in relation to 1MDB);
- reprimands; and
- warnings.

### 2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, violations of AML obligations may also be subject to criminal sanctions.

For FIs, failing to comply with its AML obligations is an offence (Section 27B(2) MAS Act) (see question 2.8). MAS may also refer matters to the CAD to evaluate whether criminal offences have been committed.

**2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?**

The relevant regulatory authority will assess the appropriate sanction(s) to be imposed based on its own guidelines and precedents. It is possible but rare to apply for judicial review of administrative decisions. An individual issued with a PO may appeal to the Minister in charge of MAS.

Typically, most resolutions of penalty actions are published by the relevant regulatory authority. MAS publishes enforcement actions against FIs and individuals on its website.

As penalty assessments are usually composition fines, FIs do not challenge such composition fines.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

FIs include:

- banks;
- merchant banks;
- finance companies;
- money changers;
- remittance agents;
- insurers;
- insurance brokers;
- capital markets intermediaries;
- trust companies;
- financial advisers;
- The Central Depository (Pte) Ltd (the Depository); and
- stored value facility holders.

Designated Businesses include:

- casino operators;
- corporate service providers;
- dealers in precious stones and/or precious metals ("**PSMD**");
- estate agents and salespersons;
- legal practitioners and law practices;
- moneylenders;
- payment service providers ("**PSP**");
- pawnbrokers; and
- professional accountants and professional accounting firms (including public accountants and accounting entities).

The applicable AML obligations are set out in specific statutes, subsidiary legislation, directions, guidelines, codes, and practice notes/circulars. Broadly, they require FIs or Designated Business to implement procedures that cover the following important areas:

- risk assessment and risk mitigation, and applying a risk-based approach;
- undertaking customer due diligence ("**CDD**") measures;
- recordkeeping requirements;
- STR requirements; and
- developing and implementing internal policies, procedures, and controls.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

Parliament passed the Payment Services Act (No. 2 of 2019) ("**PSA**") on 14 January 2019 which came into force on 28 January 2020. Under the PSA, a person carrying on a business of providing any service of dealing in digital payment tokens or any service of facilitating the exchange of digital payment tokens will have to meet AML/countering the financing of terrorism ("**CFT**") requirements under MAS Notice PSN02.

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

FIs and Designated Businesses must implement a compliance framework commensurate with their risk profile and the nature, scale and complexity of their business. This typically includes measures in relation to risk assessment and mitigation, CDD, reporting, recordkeeping, and internal policies, procedures, and controls, including ongoing monitoring of business dealings with customers (see question 3.1). Further details are in the sections below.

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

**Recordkeeping**

FIs and other Designated Businesses must retain CDD information and other data, documents and information relating to a transaction for at least five years. This may include details of its risk assessments, information on business relations with or transactions for a customer, and information pertaining to a matter that has been the subject of an STR.

FIs must retain records of financial transactions for a minimum of five years (Section 37 CDSA).

PSMDs must also maintain records of cash transactions exceeding S$20,000, as well as customer information, for a period of five years (Section 48I of CDSA).

PSPs must, to the extent possible, inquire into the background and purpose of every foreign currency exchange transaction the value of which is equal to or exceeds S$20,000 and document its findings with a view to making such information available to the authorities should the need arise.

On 11 February 2019, Parliament passed the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 ("**PSPMA**"), which came into force on 10 April 2019. The PSPMA establishes a more comprehensive supervisory and regulatory regime for a "regulated dealer" (which will include dealing in asset-backed tokens and intermediaries) to strengthen AML/CFT safeguards.

**Reporting large currency transactions**

A PSMD (or regulated dealer) must submit a CTR in respect of any cash transaction (or designated transaction), the aggregate of which exceeds S$20,000 in a transaction (or in a day) within the prescribed time (i.e. 15 days for PSMD under the CDSA). Any PSMD (or regulated dealer) who fails to comply with the above requirement shall be guilty of an offence and liable on conviction to a fine of up to S$20,000 and/or imprisonment up to two years. (Section 48J CDSA and Section 17 PSPMA.)

A casino operator is required to file a CTR with the STRO for cash transactions with a patron (or on its behalf) involving an aggregate amount of S$10,000 or more in a transaction (or in any gaming, before the end of the applicable reporting period). Any casino operator which fails to comply with the above requirement shall be guilty of an offence and shall be liable on conviction to a fine not exceeding S$20,000.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

Yes. STRs and CBNIRs are other types of reports that are filed with the STRO.

For when a STR must be filed, see question 3.9. For when a CBNI Report must be filed, see question 3.6.

**3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?**

Yes. A person who moves into or out of Singapore CBNI exceeding S$20,000 (or its equivalent in a foreign currency) must make a CBNIR in respect of the movement. A person who receives CBNI the total value of which exceeds S$20,000 (or its equivalent in a foreign currency) from outside Singapore must make a CBNI Report in respect of the receipt within five business days (Sections 48C and 48E CDSA, and regulations 2A and 4A, Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) Regulations 2007).

Certain limited exemptions are set out in Sections 48C(7) and 48C(8) of the CDSA and the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) (Exemption) Orders 2007 and 2010.

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

These include:

(a) identifying and verifying the identity of the customer (or any beneficial owner in relation to the customer);
(b) understanding the purpose and intended nature of the business relationship with the customer; and
(c) ongoing monitoring of the business relationship with the customer.

A risk-based approach is commonly adopted. Enhanced CDD measures are required for politically exposed persons (entrusted with prominent public functions) or their family members or close associates, or if business relations with or transactions for a customer presents a higher risk of money laundering. Such circumstances include (but are not limited to) where the customer or beneficial owner is from or in a country or jurisdiction in relation to which the Financial Action Task Force ("**FATF**") has identified as being high risk or which is known for having inadequate AML measures.

Enhanced CDD measures include obtaining the approval of senior management to establish or continue business relations with the customer, taking appropriate and reasonable measures to establish the customer's source of wealth and funds, and conducting enhanced ongoing monitoring of business relations with the customer.

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

Yes, FIs are prohibited from the following relationships with foreign shell banks:

- banks, finance companies and merchant banks: entering into or continuing correspondent banking or other similar services relationship (MAS Notice 626);
- capital markets intermediaries: correspondent account services relationship (MAS Notice SFA04-N02);
- money-changing or remittance business licensees: provision of remittance services (see MAS Notice 3001);
- CDP: correspondent account relations (MAS Notice SFA03AA-N01); and
- stored value facility holders: correspondent account services or other similar services relationship (MAS Notice PSOA-N02).

Each of the aforementioned FIs must also take appropriate measures when establishing the relevant relationship to satisfy itself that respondent FIs do not permit their accounts to be used by foreign shell banks.

**3.9 What is the criteria for reporting suspicious activity?**

Section 39 of the CDSA provides that a person must lodge a STR with the STRO if:

(a) he knows or has reasonable grounds to suspect that any property:
  (i) in whole or in part, directly or indirectly, represents the proceeds of;
  (ii) was used in connection with; or
  (iii) is intended to be used in connection with, any act which may constitute drug dealing/criminal conduct; or
(b) the information or matter on which the knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment.

The STR must be made as soon as is reasonably practicable after it comes to the person's attention.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

Generally, all businesses must register with ACRA. ACRA maintains this database of business entities (e.g. companies, sole proprietorships, partnerships) in Singapore and requires that the information in relation to the said entities be kept updated. Business information includes particulars of management, shareholders, secretaries, registered address, date of registration of the entity, date of change of name and/or address, issued and paid-up share capital, as well as charges held over assets of the entity (if any). Such business profiles of entities are publicly available online for purchase.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Yes. The bank ordering the wire transfer must identify the wire transfer originator and verify his identity and record adequate details of the wire transfer. In a cross-border wire transfer, the information that should be included in the payment instruction should include:

- the wire transfer originator's name;
- the wire transfer originator's account number or unique transaction reference number;
- the wire transfer beneficiary's name; and
- the wire transfer beneficiary's account number or unique transaction reference number.

Further, where the cross-border wire transfer exceeds S$1,500, additional information should be recorded in the payment instruction:

- the wire transfer originator's residential address, or registered business address (and if different, the principal place of business);
- the wire transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number); or
- the date and place of birth, incorporation or registration of the wire transfer originator (as may be appropriate).

These requirements do not apply to a transfer and settlement between the relevant FI and another FI where both FIs are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary (see paragraph 11 of MAS Notice 626, MAS Notice 824, and MAS Notice 1014, and paragraph 12 of MAS Notice 3001).

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

No (see Sections 66 and 364 of the Companies Act (Cap. 50)).

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

Yes (see question 3.1).

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

The regulatory requirements are targeted at specific industries (see question 3.1). Industries such as banks, merchants and finance companies may engage in trade finance activities. In this regard, MAS issued a Guidance Paper on AML/CFT Controls in Trade Finance and Correspondent Banking in October 2015. The objective of the paper was to provide banks, merchant banks and finance companies with guidance on the AML/CFT controls in trade finance and correspondent banking, and to share sound practices intended to help banks strengthen their controls and risk management in relation to their trade finance activities. Further, in 2018, MAS and the Commercial Affairs Department of the Singapore Police Force published a paper on Best Practices for Countering Trade Based Money Laundering pursuant to the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership formed by the two bodies in 2017.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

For the real estate sector in Singapore, Parliament passed the Developers (Anti-Money Laundering and Terrorism Financing) Act 2018 on 20 November 2018, which will come into operation on a date appointed by the Minister. As of the date of writing, no date has been appointed yet. Under this Act, property developers licensed under the Housing Developers (Control and Licensing) Act (Cap. 130) and the Sale of Commercial Properties Act will also be subject to similar AML requirements as discussed in question 3.1. This is part of government efforts to prevent the real estate industry from being used to facilitate the movement of illicit funds.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

No. In 2016, the FATF and the Asia/Pacific Group ("**APG**") on Money Laundering published a Mutual Evaluation Report of Singapore's compliance with anti-money laundering and counter-terrorist financing measures. Singapore was assessed to have either a moderate or substantial rating for effectiveness and technical compliance with 10 out of 11 immediate outcomes, and a low rating in respect of the immediate outcome for terrorism-financing investigation and prosecution. Singapore was also assessed to have either a compliant or largely compliant rating in respect of 34 out of a total of 40 FATF recommendations, and a partially compliant rating in respect of the remaining six recommendations. In 2019, FATF published a follow-up report, which revised Singapore's compliance ratings with the FATF recommendations. Under the revised ratings, Singapore was assessed to have a compliant or largely compliant rating in respect of 37 out of a total of 40 recommendations, with the remaining three being partially complaint.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The most recent evaluation was conducted by the FATF in 2019 to assess the steps taken by Singapore pursuant to the 2016 Mutual Evaluation Report. Results were published in November 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?**

The relevant AML laws, regulations, administrative decisions, and guidance can be obtained from various official websites. These include Singapore Statutes Online (http://sso.agc.gov.sg/) and MAS's website (http://www.mas.gov.sg).

**Lee Bik Wei** is the Deputy Head of the Firm's White Collar & Investigations Practice. She regularly advises clients on white-collar, regulatory and compliance and corporate governance matters, and regulatory and corporate investigations. These include matters involving criminal breach of trust, corruption, market misconduct, mutual legal assistance matters, and employee misconduct, fraud, and corporate governance-related issues.

Her main areas of practice also encompass commercial litigation and international arbitration. She has substantial experience in a range of areas including cross-border joint venture disputes, corporate disputes such as shareholder and/or directors' disputes, property and trust, and contentious employment disputes.

Bik Wei's clients include local companies and multinational corporations, both private and listed, and trust companies. Bik Wei is also proficient in Mandarin and has advised Chinese clients in arbitral proceedings.

**Allen & Gledhill LLP**
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7825
Email: lee.bikwei@allenandgledhill.com
URL: www.allenandgledhill.com

**Lee May Ling** is a Partner at the Firm's White Collar & Investigations Practice. Her key areas of practice are in corporate and commercial disputes and white-collar crimes & investigations. She has acted in a wide range of matters from multinational corporations, corporate trustees and private and publicly-listed entities.

May Ling advises companies on putting in place and managing whistleblowing and dawn raid policies and procedures. She also regularly acts for companies who are conducting internal investigations and/or are involved in investigations by enforcement authorities such as the Commercial Affairs Department, Corrupt Practices Investigations Bureau and the Monetary Authority of Singapore. This includes situations where investigations develop into criminal prosecutions by the Attorney General's Chambers.

May Ling graduated from King's College London with an LL.B. (First Class Honours) degree in 2009. She pursued an LL.M. (Commercial Law) in King's College London the following year before returning to Singapore and getting called to the Singapore Bar in 2012.

**Allen & Gledhill LLP**
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7823
Email: lee.mayling@allenandgledhill.com
URL: www.allenandgledhill.com

Allen & Gledhill is an award-winning full-service South-east Asian commercial law firm which provides legal services to a wide range of premier clients, including local and multinational corporations and financial institutions. Established in 1902, the Firm is consistently ranked as one of the market leaders in Singapore and South-east Asia, having been involved in a number of challenging, complex and significant deals, many of which are the first of their kind. The Firm's reputation for high-quality advice is regularly affirmed by strong rankings in leading publications, and by the various awards and accolades it has received from independent commentators and clients. The Firm is consistently ranked band one in the highest number of practice areas, and is one of the firms with the highest number of lawyers recognised as leading individuals. Over the years, the Firm has also been named 'Regional Law Firm of the Year' and 'SE Asia Law Firm of the Year' by many prominent legal awards. With a growing network of associate firms and offices, Allen & Gledhill is well-placed to advise clients on their business interests in Singapore and beyond, in particular on matters involving South-east Asia and the Asia region. With its offices in Singapore and Myanmar; its associate firm, Rahmat Lim & Partners in Malaysia; and its alliance firm, Soemadipradja & Taher in Indonesia, the Allen & Gledhill network has over 550 lawyers in the region, making it one of the largest law firms in South-east Asia.

**www.allenandgledhill.com**

ALLEN & GLEDHILL

# Spain


José M. Cusí


María J. Hernández


Clara Tizón

CHR Legal

## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

On one hand, the legal authorities who have powers to charge for the commission of money laundering crimes are the Public Prosecutor (judicial authority) and the State Attorney. Individuals can also charge money-laundering crimes appearing at the proceeding, known as a popular prosecution.

On the other hand, the legal authorities who have powers to investigate and to prosecute money-laundering crimes are, in the investigation phase, the Courts of Investigation and Central Courts of Investigation (when money laundering is related to certain crimes or is committed abroad); and, in the trial phase, taking into account the fact that money-laundering crimes are punished with a prison sentence of over five years in the Spanish Criminal Code (arts 301 to 303), Provincial Courts or the Criminal Section of the National High Court have powers (when money laundering is related to certain crimes or is committed abroad).

### 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 the offence of money laundering, the prosecution must prove the concurrence of acts of acquisition, possession, use, conversion or transmission of illegally obtained assets (from any crime) knowing that it or any other act aimed to hide or to conceal their illegal origin, or to help people who participated in the prior crime to avoid the legal consequences of their acts without necessarily having participated in the previous crime, and without having sentenced someone for the commission of the prior crime whenever the Judge/Court concluded that the origin of the profits was illegal. Nevertheless, constant jurisprudence has established that, to consider a money-laundering crime to have been committed, some transformation acts are required, since only the possession or use of such assets are neutral acts and are, therefore, not illegal.

Yes, tax evasion is a predicate offence 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, there is extraterritorial jurisdiction if the acts of money laundering have been committed, total or partially, abroad (art. 301.4 of the Spanish Criminal Code, "CC"), but this is a subject currently under discussion. The Supreme Court has established that, in this case, the underlying crime has to be considered as a crime in the place of commission or, at least, considered prosecutable in our system (Supreme Court Resolution, nº 974/2016).

Yes, money laundering of the proceeds of foreign crimes is punishable (art. 301.4 CC).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The authorities responsible for investigating and trying money-laundering crimes are judicial authorities. The responsibility for accusing lies with Public Prosecutors, State Attorneys and/or the popular prosecution.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

Both: penalties can be imposed on the legal entity in addition to its members.

In Spain, legal entities might have criminal liability if a money-laundering crime is committed which benefits, directly or indirectly, the company by its legal representatives, people who are authorised to take decisions on its behalf, or people who have organisational and control powers in the company; or by other members of the company who committed the crime as a result of the serious infringement of supervision, monitoring and control duties by the people aforementioned (art. 31 *bis* CC).

However, there is a criminal liability exemption for legal entities: having effectively adopted a Corporate Compliance Programme before the crime is committed. These programmes must include remedial measures in case of infringement.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Individuals: six years of imprisonment; fine equal to three times the value of the laundered assets; three years of special disqualification from the exercise of one's profession or role within their industry; and temporary (five years maximum) or definitive closing of establishments.

Also, 10 years of special disqualification from employment or public office if the crime is committed by an employer, an intermediary in the financial sector or a public officer, among others, during the exercise of their position.

Legal entities: fine for five years (maximum €5,000/day). In addition, the Judge/Court may order to close establishments, and even for the dissolution of the company.

### 1.7 What is the statute of limitations for money laundering crimes?

The statute of limitations is 10 years.

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Criminal law and enforcement of criminal offences are 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?

Firstly, there is an administrative body known as the Asset Recovery and Management Office whose function is to assist Judges and Prosecutors in locating, recovering, preserving, managing and performing the effects, assets, instruments and profits of criminal activities.

Moreover, the assets, effects and instruments confiscated as a result of the commission of a drug-dealing crime, and property confiscated as an accessory consequence for the commission of a money-laundering crime, if the assets are assigned to the State by final judgment, must be deposited at the Fund of Confiscated Assets for drug-dealing and other related crimes.

Secondly, any penalty imposed for the commission of an intentional crime, or a negligent crime with imprisonment of up to one year, must entail the confiscation of the effects that come from it, the assets, means or instruments used to commit the crime, and the profits of the crime, ordered by a Judge/Court. In addition, if it is not possible to confiscate this property, the Judge/Court will order the confiscation of other assets owned by the convicted subject with the same economic value (art. 127 CC).

Thirdly, it is possible to confiscate funds and property if there has been no criminal conviction in two cases:

- **Extended confiscation**: the Judge/Court will order the confiscation of assets, effects and profits owned by a person who is condemned for the commission of certain crimes – among them, money-laundering crimes – when it considers, based on founded objective indications (e.g. disproportion between the economic value of the assets the convicted person owns and the incomes legally obtained by him/her) that the assets or effects come from an illegal activity (committed by him/her or not) and their legal origin is not proven (art. 127 *bis* and *quinquies* CC). This is applicable when the assets come from other illegal activities of the convicted subject, other than the facts for which he is convicted, and which have not been fully proven.
- **Confiscation without criminal conviction**: the Judge/Court could order the confiscation of the property mentioned above if its illegal origin is proven through a contradictory process, and the following requirements related to the defendant have to be complied with: death or chronic illness which prevents trial; default; criminal exemption; or extinction of liability (art. 127 *ter* CC).

Forfeiture without criminal conviction, as the European Court of Human Rights has affirmed, does not have a strictly criminal nature, since it is not based on the imposition of a sanction founded on the guilt for the act. Consequently, it has a civil and patrimonial nature, close to unjust enrichment, as with extended confiscation.

Furthermore, in certain cases, the Judge/Court could order the confiscation of the aforementioned assets, effects or profits if they have been transferred to third parties (art. 127 *quater* CC).

### 1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Yes, there have been convictions of officers of banks and other regulated financial institutions, and, at this time, there are some criminal proceedings underway pursued against banks and other institutions by the Criminal Section of the National High Court for allegedly committed money-laundering crimes.

In this sense, if a legal entity is convicted, the Judge/Court may establish the prohibition of performing the activities in whose exercise the crime was committed, and even the dissolution of the company, although this has never happened yet with regards to financial institutions.

Nowadays, there are no convictions for the commission of money-laundering crimes by compliance officers, but there are some criminal proceedings underway against them for allegedly committing such crimes.

### 1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

In Spain, it is possible to settle certain criminal actions through criminal mediation, but this is not possible in money-laundering crimes as the victim of the offence is the State. Also, during the judicial process, the prosecution and defendants can settle an agreement, but only when the penalty posed by the defendant does not exceed six years of imprisonment. In this case, the defendants must express their explicit unconditional approval of the settlement reached (facts, particulars and penalty) in front of the Judge/Court, and the Judge/Court must render a judgment complying with the agreement settled if legal requirements are complied with.

No, there are no public records of such settlements. Some judicial resolutions are public through the General Council of the Judiciary webpage, and there are private webpages such as Aranzadi or Laleydigital, where some judicial resolutions are also 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 Spanish General Courts are the authority for regulating anti-money laundering law as the legislative power of the country. The Royal Decree which develops the law is approved by the Government.

The Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*, "SEPBLAC") is the Financial Intelligence Unit, the supervision authority regarding this matter, with powers to request information from the European Central Bank ("ECB") and from national regulators such as the Bank of Spain or the National Commission of the Stock Market.

The requirements are regulated in Law 10/2010, 28th April, of Money Laundering and Terrorism Financing Prevention, and developed through Royal Decree 304/2014, of 5th May. They must be complied with by individuals and legal entities that exercise some activities (such individuals are called "Obligated Subjects").

Thus, Obligated Subjects must comply with the following requirements of due diligence and previous assessment of the risk of the operation or commercial relationship:

- **Normal measures**: identification of individuals or legal entities intended to maintain commercial relationships or to participate in an operation equal to or greater than €1,000 (with exemptions) asking for reliable documentation, including identification of the beneficial owner of the legal entity involved; gathering information on whether the client acts in his/her own name or on behalf of a third party and on the structure of ownership and control of the legal entities involved; obtaining information of the purpose of the operation or relationship alleged by the client, and the nature of its commercial activity by implementing proceedings of checking the activities declared by the clients; and continuous examination of the commercial relationship.
- **Simplified measures**: clients or operations presenting little risk, e.g. public entities established in the European Union or financial entities, excepting payment entities, established in the European Union and object to examination about compliance with money-laundering requirements. Measures: identification of the client and the beneficial owner when a certain threshold is exceeded; reducing periodicity of documental reviewing; reducing monitoring of the commercial relationship and operations; and not gathering information about the activity of the client.
- **Reinforced measures**: clients or operations presenting higher risk, e.g. operations taking place or clients settled in a country which is on the OECD blacklist and when, in accordance with Spanish regulation, the country is considered to be a tax haven, or when private banking is involved or the operation involves sending money or exchanging foreign currency above certain thresholds. Also, operations related to people with public responsibilities and relatives. Measures: obtaining additional information about the origin of the assets/funds; examination and registering of the economic logic of operations; limiting the nature or quantity of the operations; and obtaining an authorisation from one directive to maintain the commercial relationship, among others.

Furthermore, Obligated Subjects have **information obligations**, i.e. implementing warnings, special examination of any fact or operation which could be related to money laundering, communicating money-laundering indications to SEPBLAC, systematic communication to SEPBLAC in some cases, to facilitate information and documentation to SEPBLAC if required, and preservation of documentation for 10 years regarding compliance with money-laundering prevention requirements and the commercial relationships maintained and operations performed.

Finally, Obligated Subjects must implement **measures of internal control**, i.e. approving and applying an Internal Prevention of Money Laundering Manual, which must include a Classification of Clients Policy, a relation of facts that could be related to money laundering, a due diligence process, etc., and designating a representative to SEPBLAC and an internal control body (in some cases); implementing a whistleblowing channel; training the members of the company on this matter and approving an annual training plan; and implementing proceedings aimed to guarantee high ethics standards in directives, employees and agents to be employed. These measures must be annually evaluated by an external expert.

**2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?**

No, there are none.

**2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?**

No. However, legal entities are responsible for the anti-money laundering compliance of its members within the entity, otherwise the company could be considered criminally or administratively liable.

Even so, legal entities could implement Corporate Compliance Programmes, which include Money Laundering Prevention rules. These programmes imply the implementation of a Disciplinary Regime, which means the company can impose disciplinary sanctions on its members if they infringe the rules settled in the Programme, regardless of the criminal or administrative liability they could have.

**2.4 Are there requirements only at national level?**

Yes, only at national level.

**2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?**

SEPBLAC is responsible for examination for compliance of anti-money laundering requirements, and the Council of Ministers, the Economy and Tax Minister, or the General Director of the Treasury are competent to impose sanctions with regards to this matter, depending on its seriousness.

Criteria of examination is publicly available on the SEPBLAC and the Commission of Money Laundering Prevention ("Commission") webpage. Furthermore, it is possible to directly send to SEPBLAC enquiries about the regulation and requirements.

**2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?**

Yes, SEPBLAC is the FIU.

**2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?**

Five years for very serious and serious infringements, and two years for minor infringements.

**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 sanction (not criminal penalties) is a fine of any of the following, whichever is highest: 10% of the net equity of the Obligated Subject; double value of the economic content of the operation; quintuple of the value of the profits of the operation; or €10,000,000 – added to a public warning or revocation of the administrative authorisation to operate.

Moreover, an administrative sanction could be imposed on directors or officers of the Obligated Subject if they are responsible for the infringement, with the maximum sanction being a fine of €10,000,000, and 10 years of professional disqualification from working for any legal entity which is an Obligated Subject or public warning.

Regarding failures, please see the following (among others):

- Very serious: not communicating an indication to SEPBLAC when it is known internally in the company; not co-operating with the authorities when is required; or resistance to inspection.
- Serious: not identifying the client, the beneficial owner, or the purpose of the business; or not continuing examination of the commercial relationship.
- Minor: infringements of legal obligations not included as very serious or serious failures.

**2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?**

The abovementioned, along with private warnings and temporary suspension of the administrative authorisation to operate.

**2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?**

The sanctions described in Law 10/2010 that could be imposed because of the infringement of anti-money laundering regulation are only administrative sanctions; there are not criminal sanctions.

As previously mentioned, the Spanish Criminal Code only punishes the use, transformation, acquisition, etc., of funds or assets which have an illegal origin, and not the infringement of the requirements of anti-money laundering, i.e. selling assets which have been obtained, for example, through selling drugs or prostitution, knowing the origin of such assets. However, it is not a crime to fail to correctly identify some clients based in a tax haven if you are an Obligated Subject; this could lead only to an administrative sanction.

In this sense, an administrative sanction cannot be imposed if the same conduct has been criminally sentenced when there is an identification of subject, facts, and legal foundations. Thus, in any moment of the administrative proceeding, if it is considered that the facts could be criminal offences, the administrative authorities must communicate this to the Public Prosecutor.

In addition, it should be noted that judicial organs must inform the Secretary of the Commission when, in the course of a judicial proceeding, they are aware of indications of non-compliance with the terms of Law 10/2010, 28th April, whenever the facts do not constitute a criminal offence.

**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 sanction procedure comprises the following phases:

- Initiation of the procedure by the Permanent Committee of the Money Laundering Prevention Commission, and notification to interested parties. This resolution must contain, among other things, the identification of the person and/or legal entity allegedly responsible and a description of the facts.
- Instruction of the procedure performed by the Secretary of the Commission. The interested parties can present allegations and evidence. Reports can be requested too.
- Imposition of the sanction by the competent authority (see question 2.5) or dismissal of the case agreed by the Permanent Committee, in a one-year maximum term. Execution of the sanction by the Secretary of the Commission.

In case of not submitting a prior declaration when it is mandatory, the administrative sanction procedure is initiated by the Secretary of the Commission, and the sanction will be always imposed by the General Director of the Treasury.

The Secretary of the Commission will inform the European Supervisory Authorities of all sanctions imposed on credit and financial institutions, including any appeal that may have been brought against them and the result.

The assessment of sanctions is made following the subsequent criteria: quantity of the affected operations; profits obtained; measures implemented to offset the mistakes or infringements; and the degree of responsibility and intentionality in the facts, etc.

The final resolution of the procedure could be appealed to the same authority (appeal for reversal) based on motives of nullity or annullability, or appealed directly to the Courts ("*contencioso-administrativo*").

a) The Commission published a list of administrative sanctions imposed in 2018, but the resolutions themselves are not public. Nevertheless, if the Obligated Subject is condemned to a public warning, the resolution is published in the Official Spanish Gazette and on the Commission webpage.

b) Yes. Banco Santander, S.A. challenged a penalty assessment in a judicial proceeding comprising an administrative sanction of a €1,000,000 fine. The sanction was confirmed by the Supreme Court of Spain.

## 3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

**3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.**

The following financial institutions and businesses performed by individuals or legal entities are subject to anti-money laundering requirements:

- Credit institutions.
- Insurance agencies and insurance agents which operate in life insurance.
- Investment service companies.
- Management companies of collective investment institutions and investment companies whose management is not committed to a management company.
- Pension fund management entities.
- Venture capital entity management companies and risk capital companies whose management is not committed to a management company.
- Mutual guarantee companies.
- Payment entities and electronic money entities.
- People who professionally perform currency exchange activities.
- Postal services regarding money order or transfer activities.
- People professionally engaged in intermediation in loans or credits granting, and people who, without authorisation as financial credit institutions, professionally perform any of these activities.
- Real estate promoters and those who professionally perform agency, commission or intermediation activities in real estate.
- Account auditors, external accountants or tax consultants.
- Public notaries and property, business and movable property registers.
- Lawyers, court agents or other independent professionals when they participate in the: conception, realisation or advising of operations on behalf of clients related the sale of real estate or commercial entities; management of funds, securities or other assets; opening or management of current accounts, savings accounts or securities accounts; organisation of the necessary contributions for the creation, operation or management of companies, or the creation, operation or management of trusts, companies or similar structures; or when acting on behalf of clients in any financial or real estate operation.
- People who professionally provide the following services on behalf of third parties: constituting companies or other legal entities; executing management or non-director secretarial functions or as an external advisory of a company, partner of an association or similar functions in relation to other legal entities; provisioning a registered office or a commercial, postal or administrative address, and other services related to a company, an association or any other legal instrument or legal entity; exercising fiduciary functions in a trust or similar legal instrument; and practising shareholder functions on behalf of another person, except companies that are listed on a regulated market in the European Union.
- Casinos.
- People who professionally trade with jewels, precious stones or metals.
- People who professionally trade with art or antique objects.
- People who professionally trade with restitution price offer assets.
- People who perform activities of deposit, custody or professional transfer of funds or payment methods.
- People who are responsible for the management, exploitation and trade of lottery or other games of luck, in physical presence or online. In the case of lotteries, mutual sports-charity bets, contests, bingos and type "B" arcade machines, this only applies with respect to prize payment operations.
- Individuals who make movements of payments methods in terms established in the Law.
- Individuals who professionally trade with assets in operations greater than €10,000 and paid by cash, cheques made payable to the bearer, or any other payment method conceived as a bearer instrument.
- Foundations and associations.
- Managers of payments systems, and compensation and liquidation of securities and financial derivatives, as well as managers of credit or debit cards issued by other entities, in terms established in the Law.
- Obligations and requirements are described in question 2.1. Even so, there is an obligation to communicate on a monthly basis to SEPBLAC some operations and the opening and cancellation of current, savings or securities accounts, or term deposits (only credit institutions).

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

Nowadays, entities within the cryptocurrency industry are not considered Obligated Subjects. However, the Directive (EU) 2018/843 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, known as "the 5th Directive", includes within the Obligated Subjects entities which are in the cryptocurrency industry. This Directive should have been transposed by Spain before 10th January 2020.

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

Spanish law does not make a distinction between companies in order to implement Corporate Compliance Programmes. It is not mandatory, nonetheless, if the company is accused of the commission of certain crimes and the Judge/Court considers that the company implemented an effective Corporate Compliance Programme before that commission; in this case, the company will be exempt from criminal liability.

The required elements of the Programme are the following: identification of the activities where crimes to be prevented could be committed; designation of a compliance officer or ethics committee; implementation of a decision-making protocol, a Disciplinary Regime and financial resources management processes; imposing the obligation to communicate possible risks or infringements of the Programme to the compliance officer; and periodic evaluation and modification of the Programme.

Even so, Money Laundering Prevention Law provides the obligation, as it is said above, of implementing internal control measures, as an Internal Money Laundering Prevention Manual, a whistleblowing channel and admission and management processes regarding clients.

Furthermore, the Spanish Stock Market Law establishes the obligation of implementing a Code of Conduct in investment services companies, among other obligations, and which includes classifying clients, transparency, monitoring conflicts of interest, information obligations, aptitude evaluation, money-laundering prevention, etc.

### 3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

There is an obligation of individuals, acting on their own behalf or on behalf of third parties, to report a prior declaration in the following cases:

- Inflows and outflows in the national territory of payment methods in an amount equal to or greater than €10,000.
- Movements of payment methods within the national territory for an amount equal to or greater than €100,000.
- Inflows and outflows in the national territory for an amount greater than €10,000 of bearer-negotiable instruments, including monetary instruments, such as travellers' cheques and negotiable instruments, including cheques, promissory notes and payment orders.

Payment methods are understood as paper and metallic currency (national or foreign), cheques made payable to the bearer, or any other payment method conceived as a bearer instrument, online or physical.

Obligated Subjects are required to monthly communicate the following movements:

- Operations involving physical movement of metallic currency, paper money, travellers' cheques, cheques or other bearer documents issued by credit institutions, except for those credited or charged to an account of a client, for an amount greater than €30,000.
- Operations performed by or with individuals or legal entities that are residents, or act on their behalf, in territories or tax havens, as well as operations that involve transfers of funds to/from said territories or countries, whatever the residence of the intervening people is, as long as the amount is greater than €30,000.

### 3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Yes, Obligated Subjects have the obligation to monthly report the following operations:

- Sending money operations involving physical movement of metallic currency, paper money, travellers' cheques, cheques or other bearer documents issued by credit institutions for an amount greater than €1,500.
- Operations which implicate payment movements subject to prior statement (see question 3.4).
- Aggregate information of sending money activity, and transfer activity within or outside credit institutions.
- Opening, modification and cancellation of current, savings or securities accounts, or term deposits (only credit institutions). The data reported will be included in the Financial Ownership File.
- Operations established by an Order of the Economy Minister.

If there are no operations susceptible to systematic communication, the Obligated Subjects have to half-yearly communicate this circumstance to SEPBLAC.

### 3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Please see the answers to questions 3.4 and 3.5.

Furthermore, regarding cross-border correspondent banking relationships with third-country entities, credit institutions have to apply the following measures: gathering information about the nature of the activities of the client, and deciding about his reputation and quality of his examination; evaluating anti-money laundering controls implemented by the client; obtaining authorisation of the management before maintaining the relationship; documenting the respective liabilities of each entity; and reinforced and permanent monitoring of the operations performed.

### 3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

Obligated Subjects must identify every client who pretends to maintain a commercial relationship with them or to participate in any operation with them, obtain information of the purpose of the operation or relationship alleged by the client and the nature of its commercial activity, and continuously examine the commercial relationship (see question 2.1).

Specifically, they must verify, before the operation is executed, the identity of the participants through reliable documents:

- Individuals: copy of his/her ID; residence card; passport, etc.
- Legal entities: certificate of incorporation; statutes; identity of the directors; tax identification number; and statement of truth of the representative of the company identifying the beneficial owner. Also, the identity of the representative must be verified asking for the powers, and the identity of the partners if the entity has no legal personality.

Moreover, depending on the type of client or activity, the following could be required to verify the activity of the client: professional association receipts; self-employed insurance receipts; tax licence; last individual income tax statement; the withholding of individual income tax; annual or trimestral VAT statement; economic activities tax statement; or other documents that justify the origin of the funds and activity.

Obligated Subjects must implement reinforced measures in case of: people with public responsibilities and their relatives; companies with shares represented by bearer instruments; clients from risk countries, territories or jurisdiction (with deficiencies in their anti-money laundering systems, tax heavens, high levels of corruption, etc.); trusts; beneficiaries of a life insurance policy; and clients that are not present.

Moreover, casinos must identify every client who accesses the establishment and who makes certain operations or transactions; associations and foundations must identify every person who receives and contributes (in this last case, an amount equal or greater than €100) funds or resources free of charge; and Obligated Subjects who manage lottery or other games of chance have to implement reinforced measures of internal control.

### 3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Any financial institution must be authorised by the Bank of

Spain prior to operating in Spain and credit institutions cannot establish or maintain correspondent banking relationships with shell banks. Also, they have to implement measures aimed to ensure that they do not establish or maintain this kind of relationship with banks which allow the use of shell bank accounts.

**3.9 What is the criteria for reporting suspicious activity?**

Facts or operations of which there is an indication or certainty of money laundering. Mainly, when the operation shows a conspicuous lack of correspondence with the nature of the operation, volume of activity or operational background of the client, as long as the special examination previously performed concludes there is no economic, professional or business justification to develop the operation.

Communications are sent by the Obligated Subject directly to SEPBLAC, prior to special examination, and there is no obligation to report to any other public institution or organism.

Obligated Subjects cannot reveal to the client or to third parties that they have communicated information to SEPBLAC, or they are examining any operation that could be related to money laundering.

Obligated Subjects have the obligation to establish internal procedures so that their members can communicate, even anonymously, relevant information about possible breaches in the prevention of money laundering. They must also adopt the appropriate measures to maintain confidentiality regarding the identity of the person who has made a communication, and he/she must be protected against retaliation, discrimination or any type of unfair treatment.

Notwithstanding the foregoing, employees, directives and agents of the Obligated Subjects can directly communicate to SEPBLAC facts or situations that could be infringements of Law 10/2010, 28th April, information that could lead to an inspection of the Obligated Subject, and every authority or public official who discovers facts that could be an indication or evidence of money laundering has the obligation to report them to SEPBLAC; otherwise, they could be sanctioned.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

Yes, there is the Public Register of Commerce where companies must maintain current and adequate information about their directors, annual accounts, statutes, etc., a National Registry of Foundations and a Centralised Body for the Prevention of Money-Laundering and Financing Terrorism of the Council of the Companies, Land and Personal Property Registrars.

Furthermore, Obligated Subjects, prior to reaching the corresponding agreement in terms established in art. 8 of the Law 10/2010, 28th April, could have access to the beneficial owner database of the General Council of Notaries, and to files which contain identification data of people with public responsibilities created by other Obligated Subjects, centralised bodies of money-laundering prevention, or third parties. Also, when certain operations have been reported to SEPBLAC and, because of their characteristics, they could be attempted in identical or similar way before others, the Commission could authorise Obligated Subjects to establish common files for exchanging information.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Yes, this is a requirement in application of the *EU Wire Transfer Regulations* (2015/847).

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

Yes, shares can be represented by bearer instruments.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

Anti-money laundering requirements are applied equally to all Obligated Subjects, with exemptions in life insurance, games of chance, foundations and associations, and for systematically communicating some information, among others, as mentioned above.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

Yes, see question 3.1 for details on Obligated Subjects.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

Spain must transpose the 5th Directive, and the transposition deadline ended on 10th January 2020.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

The follow-up assessment of anti-money laundering regulation made by FATF in 2019 establishes that almost all the measures implemented in the country have a high or substantial level of effectiveness. Only one measure has a moderate level of effectiveness, with FATF concluding that further co-operation and co-ordination between relevant investigative authorities and authorities responsible for supervising or monitoring non-profit organisations and outreach to this sector are required. Also, Spain is compliant or partially complaint with all technical measures.

The truth is, even with the approval of the Money Laundering Prevention regulations, some companies continue without complying with FATF recommendations. Recent cases have come to light, such as the Credit Suisse or Caixa Bank cases, where several subsidiaries have allegedly acted as money-laundering channels.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

Yes, by FATF in 2019. This can be found at https://www.sepblac.es/es/2019/12/05/evaluacion-de-seguimiento-de-espana-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?**

Such information can be found on the SEPBLAC webpage, within the section "Normativa": https://www.sepblac.es/es/normativa/normativa-nacional/. These materials are only available in Spanish.

**José M. Cusí** is co-founder and managing partner of CHR Legal, and he is specialised in international taxation. He graduated in law from the University of Barcelona in 1994 and has two legal Master's degrees in private and tax law. He started his professional career in 1996 at Cuatrecasas Barcelona, where he was seconded for a six-month period to the Netherlands (working at the best-friend firm Loyens & Loeff), and afterwards he was elected for a three-year period to open the Cuatrecasas New York office. Upon his return to Spain he opened and launched the tax practice area at Clifford Chance Barcelona and after another six years, he was hired by Bird & Bird in Madrid as head of tax in Spain, where he became equity partner. He returned to his hometown – Barcelona – and decided to set up his own law firm back in 2015: CHR Legal.

**CHR Legal**
Paseo de Gracia nº 74, 3º, 1ª
Barcelona (08008)
Spain

Tel: +34 931 311 444
Email: jmc@chrlegal.com
URL: www.chrlegal.com

**María J. Hernández** studied law in Madrid followed by three legal Master's degrees, and started her professional legal career as a criminal judge, a responsibility that she carried out over a 14-year period. After moving to the private sector, she was responsible for the Spanish criminal law practice of the prestigious international law firm Ontier, and afterwards she was hired by RCD (Rousaud Costas Duran) to lead the corporate compliance area on a national basis, until she decided to set up CHR Legal. Her expertise is both in preventive criminal law (i.e. corporate compliance), where she is highly ranked in *Chambers & Partners*, and reactive criminal law (i.e. criminal complaints). She has advised listed companies, large industrial groups, regulated corporations, family-owned business and private equity firms. She is also advising in some of the most relevant (economic-wise) and complex criminal court cases in Spain, such as the representation of numerous investors in Banco Popular.

**CHR Legal**
Paseo de Gracia nº 74, 3º, 1ª
Barcelona (08008)
Spain

Tel: +34 931 311 444
Email: mhe@chrlegal.com
URL: www.chrlegal.com

**Clara Tizón** studied law at ESADE faculty (2010–2014). After finishing her degree, she did a Master's in Public Economic Law and a Master's to Access to be a lawyer at the same faculty, becoming a lawyer in 2015. She started her professional career at the firm Jufresa & Grasas, and she joined CHR Legal in November 2015. She has been a member of the Criminal and Corporate Compliance Department of the firm since then.

**CHR Legal**
Paseo de Gracia nº 74, 3º, 1ª
Barcelona (08008)
Spain

Tel: +34 931 311 444
Email: ctp@chrlegal.com
URL: www.chrlegal.com

CHR Legal is a Spanish law firm founded in 2015 in Barcelona and with offices in Madrid, focused on corporate, tax and criminal law. Even though the firm is quite fresh, its three founding partners count over 25 years of experience and have worked in big law firms such as Clifford Chance, Cuatrecasas, Ernst & Young, Ontier and Bird & Bird. The firm's policy is to focus on providing added-value legal advice with a strong and steady commitment to excellence, involving always and only partners in advising clients. Among its clients, the law firm counts listed companies, large industrial groups, venture capital and private equity firms, family-owned business and family offices as well as high-net-worth individuals. The firm is outlined in the main legal directories, such as *Chambers & Partners* and *BestLawyers*, and the main contact and managing partner is José María Cusí.

**www.chrlegal.com**

# Switzerland


Dr. Omar Abo Youssef


Lea Ruckstuhl

Kellerhals Carrard



## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the 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 has still applied to so-called qualified tax offences relating to direct taxes (*cf.* question 1.1 above).

Among Swiss law experts there is a dispute as to whether the new offence of money laundering in tax matters is indeed functional, since avoidance of taxes in principle (i) triggers no forfeiture, but just a supplementary tax assessment, and (ii) does not lead to the acquisition of specific assets which originate from the qualified tax offence and could be forfeited.

### 1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

If the predicate offence – in other words the felony or the qualified tax offence – was committed abroad and is punishable there, then the perpetrator shall be prosecuted and punished in Switzerland for the money laundering committed in Switzerland (art. 305*bis* no. 3 SCC). This provision serves to protect the foreign forfeiture claim. Applying the provision to foreign predicate offences can therefore be problematic if a foreign state does not know the concept of forfeiture of specific (tainted) assets, but rather absorbs tortious benefits exclusively by means of a claim for compensation (see also question 1.9 in this regard).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Depending on whether the money laundering is directed against the Federation's or the Canton's administration of justice, criminal proceedings for money laundering are conducted either by the Federal Prosecutor's Office or by the cantonal public prosecutor's offices (art. 23 para. 1 *lit.* h of the Swiss Code of Criminal Procedure [SCP]). If money laundering is, to a large extent, carried out abroad or in several cantons without being concentrated in one canton, then the Federal Prosecutor's Office shall be responsible for prosecution (art. 24 para. 1 SCP). However, under certain conditions the Federal Prosecutor's Office can transfer a criminal case that falls under its jurisdiction in accordance with art. 23 SCP to the cantonal prosecutor's offices for investigation (art. 25 SCP).

The Money Laundering Reporting Office Switzerland (MROS) similarly plays an important role in the prosecution of money laundering. It receives reports from financial intermediaries who transmit them by virtue of their reporting rights or their reporting obligation, and subsequently reviews and analyses them (see question 2.6). It notifies the relevant prosecuting authority if it has reason to suspect that money laundering has taken place or that assets originate from a felony or a qualified tax offence in accordance with art. 305*bis* no. 1*bis* SCC.

Any violations of the reporting obligation (art. 37 of the Federal Act on Combating Money Laundering and Terrorist Financing [AMLA]) are prosecuted by the Federal Department of Finance (art. 50 para. 1 of the Federal Act on the Swiss Financial Market Supervisory Authority [FINMASA]). For more details about the reporting obligation, please see question 3.9.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

In Switzerland, both natural persons and companies can be prosecuted and convicted for money laundering. In accordance with art. 102 para. 1 SCC, any felony or misdemeanour committed in a company in the exercise of commercial activities in accordance with the objects of the company is attributed to the company if that act cannot be attributed to any specific natural person due to inadequate organisation of the company (subsidiary corporate liability).

In accordance with art. 102 para. 2 SCC, the company shall be punished independently or in addition to the criminal liability of any natural persons if the felony or misdemeanour involves certain offences, including in particular money laundering, and if the company has failed to take all the reasonable organisational measures in order to prevent such an offence (cumulative corporate liability).

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

In the event of natural persons being convicted in accordance with art. 305*bis* no. 1 SCC, the maximum prison sentence is three years. In qualified cases (art. 305*bis* no. 2 SCC), in particular, if the perpetrator is acting as a member of a criminal organisation or as a member of a group that has been formed for the purpose of the continued conduct of money-laundering activities, or if he/she achieves, by means of commercial money laundering, a large turnover or a substantial profit, then the maximum prison sentence shall be five years, combined with a maximum monetary penalty of 500 daily penalty units of up to CHF 3,000 each.

If a company is convicted of money laundering, the maximum fine shall be CHF 5 million (art. 102 para. 2 in conjunction with para. 1 SCC).

### 1.7 What is the statute of limitations for money laundering crimes?

The limitation period for prosecution is 10 years (art. 97 para. 1 *lit.* c SCC) for the basic offence of money laundering (art. 305*bis* no. 1 SCC) and 15 years (art. 97 para. 1 *lit.* b SCC) for the qualified offence (art. 305*bis* no. 2 SCC). As money laundering is an ongoing offence, the limitation period for prosecution begins on the day on which the criminal conduct ceases (art. 98 *lit.* c SCC). The limitation period for prosecution ceases to apply if a judgment by a court of first instance has been issued before the limitation period for prosecution has expired (art. 97 para. 3 SCC).

It should be noted that the limitation period for prosecution of the predicate offence also plays a role. If the predicate offence is barred by a statute of limitation, then no forfeiture or money laundering in terms of frustrating the forfeiture will be possible. The limitation period for prosecution of predicate offences (felonies and qualified tax offences) is 15 years.

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

There are no money-laundering provisions in Switzerland on a cantonal or municipal level. Only art. 305*bis* SCC applies. However, criminal proceedings for money laundering are also prosecuted by the cantonal prosecutors (see question 1.4).

### 1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

In accordance with art. 70 para. 1 SCC, the court orders the forfeiture of assets that have been acquired through the commission of a criminal offence, unless the assets are passed on to the person harmed for the purpose of restoring the prior lawful position.

Forfeiture shall only be precluded if a third party has acquired the assets in ignorance of the grounds for forfeiture and has (cumulatively) provided an equivalent consideration for them, or if forfeiture would otherwise cause him disproportionate hardship (art. 70 para. 2 SCC).

The objects of forfeiture are assets obtained directly or indirectly by means of a criminal offence. These must have a natural and adequate causal link to the criminal offence, but do not necessarily have to be the direct and immediate consequence of the offence. For example, income from legal transactions that have been concluded based on bribery can also be confiscated. It is undisputed that surrogates of assets acquired through a criminal offence can be confiscated as well.

If the assets which are subject to forfeiture no longer exist, e.g., because they have been consumed or disposed of, then the court orders a compensation claim for the same amount (art. 71 para. 1 SCC). The compensation claim may be enforced in any assets, including assets which may have been legally acquired. Frustrating the compensation claim does not qualify as money

laundering since it does not focus on "tainted" assets. Money laundering applies only to frustrating the forfeiture of "tainted" assets that are proven to be directly or indirectly derived from a felony or a qualified tax offence.

It is an issue of controversy whether the scope of the benefit to be recovered should be determined on a net or gross basis. For generally prohibited activities (e.g., drug trafficking), gross calculations apply, whereas for acts that are permitted in principle, but are only tortious in specific instances (e.g., a contract that has been obtained through corrupt means), net calculations are used, i.e. the production costs are deducted.

Law enforcement authorities may order the provisional seizure of assets if they are likely to be forfeited or serve to enforce the compensation claim (art. 263 para. 1 *lit.* d SCP, art. 71 para. 3 SCC).

As forfeiture and compensation claims involve objective measures and not penalties, these sanctions are applied regardless of the criminal liability or conviction of a particular person. This is on the condition, however, that all objective and subjective elements of the underlying offence can be proven and that there is no general defence.

**1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?**

Yes. It is worth mentioning, for example, the conviction of bank officers for money laundering by omission (BGE 136 IV 188). The relevant case was based on the following facts: the bribes received by tax officials from the District of Rio de Janeiro were transferred to accounts of a bank headquartered in Geneva. Although the question of the admissibility of a PEP engaging in secondary employment did relate to one of the officials, internal transfers to other tax officials did take place and the accounts showed a rapid increase in capital, thus the evidence suggested that the tax officials' balances could be of criminal origin; the bank officers neglected to inform the bank's general management. As a result of this omission, they breached the duties of care incumbent on them and prevented the accounts from being reported to MROS and being blocked.

Another ruling of the Federal Supreme Court relates to the criminal liability of a bank for lack of organisational measures to prevent money laundering (BGE 142 IV 333). The decision was based on the following facts: after the transfer of EUR 5 million to an account at the bank – the transfer was based on fraud – the amount of CHF 4.6 million was withdrawn in cash. The Federal Supreme Court denied the bank's cumulative liability for money laundering since the necessary conditions, i.e. the underlying criminal liability of a natural person for money laundering, was not established. The case shows that the cumulative liability of companies for money laundering is indeed cumulative and not strict liability.

**1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?**

Switzerland does not know plea agreements as they occur, e.g., in the U.S. However, criminal prosecution may be abandoned in certain circumstances, in particular if the offender has made reparations (art. 53 SCC). In this regard, reference should be made to the abandoning of corruption proceedings against a French company on the basis of art. 53 SCC, after it had made reparations to the value of CHF 1 million. At the same time, however, the Swiss subsidiary of the same concern was sentenced, by means of a summary penalty order, to a fine of CHF 2.5 million as well as a claim for compensation to the value of CHF 36.4 million.

In accordance with Federal Supreme Court case law, orders for abandoning prosecutions can be inspected if there is a legitimate interest in the information and it is not opposed by any overriding public or private interests.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

**2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.**

The basic principles for combatting money laundering are laid down in the Federal Act on Combating Money Laundering and Terrorist Financing (AMLA). The scope of application of the AMLA as well as the duties for the traders are clarified in the Anti-Money Laundering Ordinance of the Federal Council.

The obligations for the prudentially supervised financial intermediaries (especially banks) are specified in the Anti-Money Laundering Ordinance of the Swiss Financial Market Supervisory Authority (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 Swiss Financial Market Supervisory Authority (FINMA), the self-regulatory organisations, the Federal Gaming Board, or the supervisory commission of the Swiss Bankers Association for its Code of Conduct with regard to the exercise of due diligence (CDB) (see questions 2.2 and 2.3). Reference is hereby made to questions 3.1 and 3.7 for the requirements related to combatting money laundering. It should be noted that since 1 January 2020, the status of DSFIs, financial intermediaries pursuant to art. 2 para. 3 AMLA, which are directly subordinated to the FINMA and supervised by FINMA, has been abolished.

Under the Swiss legislation until the end of 2019, the so-called "independent asset managers" have not been subject to prudential supervision, besides the AMLA subordination, which was necessary, if they have engaged in asset management professionally. This lack of prudential supervision was not in line with European Union Law. Therefore, and to achieve equivalence with MIFID II, the Financial Services Act (FinSA) and the Financial Institutions Act (FinIA) were adopted and came into force on 1 January 2020. The biggest novelty in the FinSA and the FinIA is the authorisation obligation incumbent on asset managers. While FINMA alone is responsible for the authorisation of the independent asset managers, the supervision is carried out by a supervisory body. The supervisory body is separate and independent from FINMA, but is itself authorised and supervised by FINMA. Regardless of FinSA/FinIA, the duty of each independent asset manager to comply with AMLA remains in force. However, according to current knowledge, all supervisory bodies will also operate as self-regulatory organisations.

**2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?**

Supervision of financial intermediaries under art. 2 para. 3 AMLA is exercised through the self-regulatory organisations.

With regard to independent asset managers, it is probable that the supervisory body will also operate as a self-regulatory organisation. This ensures that AMLA supervision can be carried out hand in hand with FinIA supervision.

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.

The supervisory bodies which will probably also perform anti-money laundering compliance against their members are allowed to perform the ongoing supervision. FINMA reserves the right to issue decrees, and enters into the ongoing supervision of the supervisory body if this is necessary to enforce the financial market laws pursuant to art. 1 para. 1 FINMASA.

### 2.4 Are there requirements only at national level?

Yes, requirements are only at national level.

### 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

FINMA is responsible for monitoring the prudentially supervised financial intermediaries (especially the banks). Furthermore, FINMA enters into the ongoing supervision of the supervisory body if this is necessary to enforce the financial market laws pursuant to art. 1 para. 1 FINMASA. The self-regulatory organisations are responsible for enforcing the requirements *vis-à-vis* their affiliated financial intermediaries. The independent asset managers receive ongoing supervision by their supervisory body.

It should be emphasised that the banks, in addition to FINMA, are also supervised by their professional organisation's supervisory committee.

FINMA publishes the procedure in connection with auditing in the context of circulars, as well as various information on so-called "enforcement proceedings".

### 2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

The Money Laundering Reporting Office Switzerland (MROS) at the Federal Office of Police is the national central office which examines suspicious transaction reports, analyses them and, if necessary, forwards them to the relevant law enforcement authorities.

### 2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

By virtue of art. 52 FINMASA, the prosecution of any violations of this law and of the financial market laws has a limitation period for prosecutions of seven years.

### 2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Self-regulatory organisations do not have a homogeneous fine policy and the fines vary in terms of amount. The Swiss Bankers Association's Supervisory Commission may, for example, issue penalties of up to CHF 10 million. The offences that can lead to fines or penalties are specified in the corresponding regulations. FINMA itself does not have any authority to issue fines. However, FINMA may take other measures, such as confiscating profits.

### 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 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, for example, professionally lend or provide payment services.

In June 2019, the Swiss Federal Council adopted the dispatch on the amendment of the AMLA. This amendment includes measures for persons providing services in connection with domiciliary companies or trusts (advisors). The advisers have to comply with the due diligence obligations and will also have a reporting duty to the FIU. Parliament will be addressing these measures in 2020.

Please refer to question 3.7 for a description of the due diligence obligations.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

FINMA assesses money-laundering risks as especially high in a decentralised blockchain-based system, where assets can be transferred anonymously and without regulated intermediaries.

In February 2018, FINMA published guidelines regarding initial coin offerings (ICOs). Based on these guidelines, FINMA focuses on the economic function and purpose of the token issued by the ICO organiser. Relevant is the underlying purpose of the token and if they are tradeable or transferable. FINMA distinguishes between payment tokens, utility tokens and asset tokens. If the ICO issues already existing payment tokens, it is qualified as a means of payment and subjected to the AMLA. Either the ICO organiser affiliates itself to an SRO and fulfils the AMLA obligations itself (e.g. identifying the contracting party) or these requirements can be fulfilled – exceptionally – through "delegation", by having the funds accepted via a financial intermediary, which is already subject to the AMLA and who exercises the corresponding customer due diligences for the ICO organiser.

The ICO of utility tokens or asset tokens are not qualified as means of payment under the AMLA and are therefore not subjected to the AMLA.

Under current FINMA practice, the exchange of a cryptocurrency for fiat money or a different cryptocurrency falls under art. 2 para. 3 AMLA. The custodian wallet provider, the online exchange office and the centralised trading platform are subject to the AMLA as well.

Furthermore, it must be noted that in September 2018, the Swiss Bankers Association published guidelines for its members regarding opening corporate accounts for blockchain companies.

In September 2019, FINMA published a supplement to the guidelines for enquiries regarding the regulatory framework for ICOs. In this document, FINMA makes an indicative classification under supervisory law for "stable coins". Due to their frequently intended purpose as a means of payment, the AMLA mostly applies to "stable coins". Projects relating to create "stable coins" may result in the application of the Banking Act or the Collective Investment Schemes Act. If a payment system of significant importance is launched, a licensing requirement as a payment system is probable under the Financial Market Infrastructure Act (FinMIA).

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

AMLO-FINMA sets specific requirements for certain types of financial intermediaries. Art. 20 para. 2 AMLO-FINMA should be mentioned, for example, which stipulates that banks and securities dealers must operate a computer-based system for monitoring transactions. Such system will help to identify transactions with increased risks.

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

All documents required in connection with the fulfilment of the due diligence obligations must be kept for 10 years after the business relationship in question has been terminated or the transaction has been carried out (art. 7 para. 3 AMLA). There is no obligation, however, to automatically report large currency transactions to the FIU.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

There are at present no automatic reporting requirements to the FIU in Switzerland for any transactions.

### 3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

There is no obligation to automatically report cross-border transactions to the FIU.

### 3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

1) Identifying the contracting party: A financial intermediary must identify the contracting party on the basis of a valid document (e.g. passport or extract from the commercial register) when commencing a business relationship.
2) Establishing the identity of the beneficial owner of the assets: In the case of natural persons, the financial intermediary must determine whether there are any doubts about the principle that the contracting party is also the beneficial owner of the assets. Since 1 January 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 the "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 anti-money laundering training, and makes the necessary reports to the Money Laundering Reporting Office, if this duty has been delegated from the supreme management body to the anti-money laundering department.
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).

The dispatch on the amendment of the Anti-Money Laundering Act (AMLA) states that in future, the beneficial owner must not only be established but also verified. It is still unclear how this verification is to be carried out in concrete terms.

The draft law also states that client data must be updated regularly. The financial intermediary can in principle proceed on a risk-based approach. Legal requirements that have come into force since the beginning of the business relationship must also be taken into account. It should be noted that the draft law will be debated in Parliament in 2020 and that changes may therefore still occur.

### 3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

In accordance with art. 8 *lit.* b AMLO-FINMA, the financial intermediary may not start any business relationships with banks that have no physical presence at the place of incorporation (foreign shell banks), unless they are part of an appropriately consolidated supervised financial group.

### 3.9 What is the criteria for reporting suspicious activity?

A financial intermediary must immediately notify the Money Laundering Reporting Office if it knows, or has reasonable grounds to suspect, that the assets involved in the business relationship are related to a criminal offence under art. 260*ter* number 1 (criminal organisation) or art. 305*bis* SCC (money laundering), are the proceeds of a felony or a qualified tax offence, are subject to the power of disposal of a criminal organisation or serve the financing of terrorism (art. 260*quinquies* para. 1 SCC). Furthermore, the financial intermediary shall have a duty to report if it cancels negotiations for commencing a business relationship based on a reasonable suspicion of this nature. Finally, the financial intermediary shall also be required to report, in accordance with the provisions of art. 6 para. 2 *lit.* d AMLA, if he 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).

MROS and FINMA have developed a practice in connection with the reporting obligation of the financial intermediary. Pursuant to this practice: "reasonable suspicion exists when the results of these clarifications fail to refute the suspicion that the assets are linked with a crime. The financial intermediary must report such business relationships to MROS (duty to report under Article 9 AMLA; see decisions of the Swiss Federal Criminal Court SK.2017.54 of 19 December 2017 and SK.2014.14 of 18 March 2015, consid. 4.5.1.1). If it is unclear whether a report must be filed, the financial intermediary may still do so (reporting right in accordance with Article 305*ter* para. 2 SCC)." (Please refer to https://www.finma.ch/en/documentation/dossier/dossier-geldwaeschereibekaempfung/rechtsprechung-und-praxis-zur-meldepflicht/.) The difference between the reporting duty and the right to report will be clarified at ordinance level as part of the ongoing revision of the AMLA.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

Currently, there is no publicly accessible register that contains information about the beneficial owners of an operating legal entity who ultimately control the legal entity. However, there is a commercial obligation to keep a register of bearer shareholders and beneficial owners of the bearer and nominal shares.

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Yes. Based on art. 10 of the AMLO-FINMA, the payer's financial intermediary for the payment order must state the name, the account number, and the address of the payer as well as the beneficiary's name and the account number. There are certain easements for payment orders within Switzerland.

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

The Federal Council has introduced new regulations as of 1 November 2019, and the heart of this legislative reform is the abolition of bearer shares for privately held companies limited by shares. Basically, bearer shares are no longer permitted in Switzerland. The only exceptions are bearer shares of listed companies and bearer shares structured as intermediated securities. These new regulations are linked to the recommendations of the Global Forum. Switzerland was recommended to tighten its transparency requirements regarding legal entities (especially related to bearer shares), which were introduced in 2015.

The listing/structuring of the shares as intermediated securities must be requested from the Commercial Register by 1 May 2021. If no entry has been requested by that date, and if a company limited by shares still has bearer shares at that point, these will be converted by law into registered shares. The shares of bearer shareholders who fail to make the required notifications to the Company during the transition periods will become null and void.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

No. However, if a trader carries out a transaction of CHF 100,000 in cash, it must then comply with the limited due diligence and reporting obligations under art. 17 *et seq.* of the Anti-Money Laundering Ordinance of the Federal Council.

The amendment of the AMLA will be discussed in Parliament in Switzerland during 2020. This amendment includes measures for persons providing services in connection with domiciliary companies or trusts (for example lawyers). It can be assumed that the scope of application of the AMLA will be extended in the future and also includes non-financial institutions.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

No, there are not.

## 4 General

**4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?**

Due to the fact that Switzerland narrowly failed the FATF country evaluation in 2016 and is in the so-called enhanced follow-up, a duty on the part of the financial intermediary to verify the customer's information on the beneficial owner and an event-independent obligation for the regular updating of the customer documentation shall be introduced. In addition, discussions are underway to lower the threshold for the reporting obligation, so that financial intermediaries will, in future, have to report in the event of mere simple suspicion on the basis of art. 9 AMLA.

In June 2018, the Federal Council of Switzerland published a legislative draft amending the AMLA. The scope of the AMLA should be extended and due diligence obligations are to be introduced for certain services which concern the establishment, management or administration of domiciliary companies with a registered office in Switzerland or abroad and trusts. This amendment especially focuses on lawyers and notaries and will also apply the AMLA duties (in amended form) to them. Furthermore, associations which are at risk of being misused for terrorism or money laundering must be entered in the commercial register. In June 2019, the dispatch on the amendment of the AMLA was adopted by the Federal Council. The amendment of the AMLA will be discussed in Swiss Parliament during 2020. The measures are not expected to come into force until the start of 2021 at the earliest.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

See question 4.3.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

On 7 December 2016, the fourth FATF Country Report for Switzerland was published. Switzerland scored well for the legal mechanisms, and was rated as "compliant" or "largely compliant" for 31 of the 40 recommendations. With regard to the effectiveness of the legal provisions, Switzerland scored high in seven out of the 11 subject areas examined. Switzerland achieved above-average results in comparison to the other countries that have already been audited.

However, this does not change the fact that Switzerland did fail the country evaluation, like many other countries. This is especially the case because, according to the FATF, Switzerland's

efforts in connection with establishing the identity of the beneficial owner and especially with verifying this information have been insufficient to date. There is, therefore, a need for action in the area of technical compliance, in other words primarily at the level of the AMLA and the regulations and rules issued by the SRO. It is expected that a duty to verify the information on the beneficial owner, as well as a regular and event-independent obligation to update customer information, will be introduced. The relevant revisions are under consideration or already in progress (see question 4.1 above). The report about Switzerland can be downloaded at https://www.fatf-gafi.org/media/fatf/content/images/mer-switzerland-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?**

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.
- Information on the Financial Services Act (FinSA) and the Financial Institutions Act (FinIA) are available under https://www.finma.ch/en/authorisation/fidleg-und-finig.

## Acknowledgment

The authors would like to acknowledge Florian Baumann, Responsible Partner, for his contribution to this chapter. Florian is head of the Kellerhals Carrard White Collar Crime practice group and represents clients in multinational asset recovery cases, criminal and administrative legal assistance proceedings and internal investigations. He advises banks and other financial intermediaries on compliance issues, including representation in administrative investigations or compliance-related litigation.

**Dr. Omar Abo Youssef** is a member of Kellerhals Carrard's White Collar Crime practice group. He graduated from the University of Zurich (*Juris Doctor* and Master of Law) and Geneva (Certificate of Transnational Law) and is admitted to all Swiss courts. He lectures in criminal law and criminal procedural law at the University of Zurich and is chairman of the Schulthess Conference on White Collar Crime. Omar specialises in complex criminal, regulatory and civil litigation matters, with a special focus on white-collar crime, international assistance in criminal matters and asset recovery. Omar 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.

**Kellerhals Carrard**
Rämistrasse 5
PO Box, 8024 Zürich
Switzerland

Tel: +41 58 200 39 00
Email: omar.aboyoussef@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

**Lea Ruckstuhl**, senior associate, is a member of Kellerhals Carrard's White Collar Crime practice group. She graduated from the University of Freiburg in 2007 with the addition of European law ("*summa cum laude*") and received the Frilex Prize for the best university degree. Lea is admitted to all Swiss courts.
As head of the department of the self-regulatory organisation for the Swiss Leasing Association (SRO/SLV), she has broad experience in the field of leasing and financing. Her main areas of practice include financial market supervision (non-banks and insurance companies), in particular in the field of combatting money laundering. She is also a member of the Audit and Investigation Body of the self-regulatory organisation of the Swiss Insurance Association and a member of the Board of Directors of the Association Forum SRO. Lea frequently gives presentations in her field of activity and is co-author of a 2017 published book about compliance.

**Kellerhals Carrard**
Rämistrasse 5
PO Box, 8024 Zürich
Switzerland

Tel: +41 58 200 39 00
Email: lea.ruckstuhl@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

With more than 200 professionals (comprised of partners, salaried lawyers, legal experts, tax advisers and notaries) and a total of more than 300 staff, the law firm Kellerhals Carrard, which dates back to 1885 and has offices in Basel, Berne, Geneva, Lausanne, Lugano, Sion and Zurich and representation offices in Binningen, Shanghai and Tokyo, is the second largest in Switzerland and boasts a rich tradition.
Kellerhals Carrard operates throughout Switzerland, whilst maintaining very strong local roots, advising clients nationally and abroad. The firm advises and represents companies and entrepreneurs from all industries and economic sectors, public authorities, national and international organisations and private individuals before all judicial and administrative bodies nationally and abroad in practically all areas of the law.
In recent years, governments have increased their efforts and adapted their laws and regulations in order to fight fraud, corruption, money laundering, financing of criminal activities and terrorism. As a result, criminal law is increasingly important for international business and finance.

Over the years, Kellerhals Carrard has developed a substantial practice in the field of national and transnational commercial criminal law. The firm's attorneys have also been closely involved in developments in this field through their lecturing activities and publications. Kellerhals Carrard's Investigation, Compliance and White Collar Crime team consists of 27 lawyers.

**www.kellerhals-carrard.ch**

Kellerhals Carrard

# United Kingdom



John Gibson


Tim Harris

Cohen & Gresser (UK) LLP


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the 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 (ss 327–329); and
- the reporting offences which, with one exception, only apply to those operating in the "regulated sector" (ss 330–332).

It is also an offence 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 Part 2 of the Terrorism Act 2000. The anti-terrorist financing regime in the UK runs parallel to the UK's anti-money laundering regime.

Of relevance to regulated firms, the UK has a regulatory framework, principally underpinned by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (**MLR 2017**) as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (**MLR 2019**), which transposed the Fifth Money Laundering Directive (**5MLD**) into UK law. The MLR 2019 came into force on 10 January 2020. The MLR 2017 apply to regulated firms and individuals, principally financial institutions but also lawyers conducting transactional work, accountants, tax advisers, estate agents, art market participants and others. The MLR 2017 impose certain requirements relating to customer due diligence, policies and procedures, controls, and recordkeeping amongst other things. All regulated firms should comply with the MLR 2017. Failure to do so is a criminal offence.

### 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 (s.327 POCA);
  (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 (s.328 POCA); or
  (iii) acquired, used or had possession of criminal property (s.329 POCA); 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" (defined in s.340 POCA) 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 constitutes or represents such a benefit (this is a subjective limb).

The test for "criminal property" requires there to be "criminal conduct" and, accordingly, there must be a predicate offence in order for criminal property to exist. As a result, the money laundering offences are sometimes referred to as being parasitic. Conduct (wherever carried out) 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 (**CFA**) introduced two new corporate failures to prevent the facilitation of tax evasion offences. These are strict liability offences, committed when a person who performs services for or on behalf of a company facilitates UK or foreign tax evasion. The company may have a defence if it can prove that it had reasonable procedures in place to prevent the facilitation. These offences are predicate offences for money laundering.

**Reporting offences**

Reporting offences include the failure to disclose, tipping-off and prejudicing a money laundering investigation.

It is an offence for those acting in the regulated sector not to report money laundering. To establish that a failure to disclose an 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;

(b) the information or other matter on which that knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, 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; 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).

There is also a reporting offence for nominated officers other than those working in the regulated sector.

The tipping off offence is also relevant to those acting in the regulated sector. To establish that an 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.

This offence can be committed by anyone.

### 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.

What is less clear is whether POCA is engaged where both the predicate and the money laundering offence take place outside the UK and the only UK nexus may be that the firm's compliance or investigative team are located in the UK. In these circumstances, there are some doubts about the jurisdictional scope of the money laundering provisions but, as the law stands at present, POCA criminalises acts of laundering that take place anywhere in the world. Note some professional guidance indicates that failure to make a disclosure where all suspected predicate offending occurs outside the UK and there is otherwise no UK nexus to the suspected criminality may constitute a "reasonable excuse" not to make a disclosure.

A person will not commit a principal money laundering offence if:
(a) he/she knew, or believed on reasonable grounds, that the relevant conduct occurred in a country or territory outside the UK; and
(b) the relevant conduct:
  (i) was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory; and
  (ii) does not constitute an offence punishable with imprisonment for a maximum term in excess of 12 months in any part of the UK if it had occurred there.

There are also similar overseas conduct defences in relation to the disclosure offences.

The CFA expanded the definition of "unlawful conduct" in Part 5 (civil recovery) POCA to include overseas conduct that constitutes (or is connected with) the commission of a gross human rights abuse or violation. Provided that the conduct, if it occurred in a part of the UK, would be unlawful under the criminal law of that part of the UK, there is no requirement for the conduct also to be unlawful overseas.

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Money laundering offences are usually investigated by the National Crime Agency (**NCA**), the police, or Her Majesty's Revenue and Customs (**HMRC**). As a rule, money laundering offences are prosecuted by the Crown Prosecution Service. However, there are exceptions to this; for example, cases involving serious fraud or corruption are likely to be investigated and prosecuted by the Serious Fraud Office and, as the financial services regulator, the Financial Conduct Authority (**FCA**) has the power to investigate and prosecute offences under POCA or MLR 2017 falling within its remit.

### 1.5 Is there corporate criminal liability or only liability for natural persons?

Corporate entities can be criminally liable for money laundering offences subject to the rules for attributing criminal liability to corporate entities. The money laundering offences in POCA and MLR 2017 apply to corporations as well as individuals.

### 1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

Different offences under POCA have different maximum penalties. The highest maximum penalty is 14 years' imprisonment (for individuals) and/or an unlimited fine (applicable to both individuals and corporations).

An offence under MLR 2017 is punishable by up to two years' imprisonment (for individuals) and/or an unlimited fine (applicable to both individuals and corporations).

### 1.7 What is the statute of limitations for money laundering crimes?

There is no time limit in respect of which criminal conduct can

give rise to criminal property, and accordingly, prosecutions can be brought at any time. However, offences under POCA cannot be committed retrospectively and money laundering offences committed before the commencement of POCA will be prosecuted under the previous legislation.

**1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?**

Broadly speaking, enforcement is at a national level. Part 7 of POCA (which, as noted above at question 1.1, contains the principal money laundering offences) applies equally throughout the UK, although there are separate (but similar) provisions for confiscation and restraint procedures in Scotland and Northern Ireland.

Note that the NCA's operational powers in Scotland are conditional on authorisation from the Lord Advocate.

**1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?**

Yes, there is a confiscation regime under POCA. A confiscation order deprives an individual – who has been convicted of a money laundering offence (or any other criminal offence) – 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.

Other than criminal conviction, there are a number of civil and summary processes that law enforcement can use to recover assets they allege are the proceeds of crime. Part 5 of POCA contains powers that enable an enforcement authority to pursue a civil recovery order in the High Court, which facilitates the recovery of proceeds of crime without the need for a conviction. The Court must be satisfied that the property in question is or represents the proceeds of unlawful conduct. Although not included within Part 5, Unexplained Wealth Orders are a well-publicised disclosure tool inserted into POCA by the CFA, which require the respondent to provide information and documents about property including how the property was obtained. Once this information has been received the authority may pursue recovery of the property through the civil recovery process.

Enforcement authorities can also seek to freeze and forfeit cash held in bank and building society accounts and seize and forfeit physical cash in summary proceedings.

**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 or the MLR 2017. At the time of writing, the FCA is investigating a number of firms for money laundering on a "dual track" that might give rise to either criminal or civil proceedings. Mark Steward, the FCA's Director of Enforcement, said in a speech on 4 April 2019 that he suspected "criminal prosecutions, as opposed to civil or regulatory action, will be exceptional. However, we need to enliven the jurisdiction if we want to ensure it is not a white elephant and that is what we intend to do where we find strong evidence of egregiously poor systems and controls and what looks like actual money-laundering".

In September 2019, an individual was convicted for laundering the proceeds of a conspiracy to insider deal for which a regulated corporate broker had been previously convicted.

There have been a small number of individuals convicted for the failure to report offence – including at least three solicitors. None were employed by banks.

**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 criminal justice system. 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 (contained in decision notices) are usually made public. Recent notable examples include:

In April 2019, Standard Chartered Bank was fined £102.2 million for AML breaches in 'higher risk' areas of its overseas business.

In July 2018, Canara Bank was fined £896,000 and restricted from accepting deposits for 147 days for failing to maintain effective AML systems and controls between 2012 and 2016.

In January 2017, Deutsche Bank was fined £163 million for failing to maintain an adequate AML framework between 2012 and 2015.

## 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. AML compliance is dealt with in Senior Management Arrangements, Systems and Controls (**SYSC**) and in particular SYSC 3.2.6.

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.

The Solicitors Regulation Authority (**SRA**) requires individuals and firms respectively to make sure they keep up to date with, and remain aware of, their responsibilities under any new legislation as and when it is introduced.

### 2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

The three statutory AML supervisors are HMRC, the Gambling Commission and the FCA (within which sits the Office for Professional Body AML Supervision (**OPBAS**)). OPBAS has duties to ensure that the 22 supervisors of accountancy and legal professionals (including the Institute of Chartered Accountants in England and Wales, the Law Society of England and Wales and the SRA) meet the standards of the MLR 2017.

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. OPBAS 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 2019 the Solicitors Disciplinary Tribunal penalised two solicitors for AML failings:

a) in July 2019, a solicitor targeted by criminals to facilitate 'dubious investment transactions' was struck off. He was held to have failed to carry out appropriate customer due diligence in accordance with money laundering regulations; and
b) in January 2019, a solicitor was fined £45,000 for failing to carry out basic AML background checks. Costs of £40,000 were also imposed.

As of May 2019, the SRA reported that it was probing 26 law firms over alleged money laundering breaches, chiefly in relation to carrying out inadequate risk assessments.

### 2.4 Are there requirements only at national level?

The MLR 2017 operates at the national level. Equally, the FCA is the regulator for the financial sector across the UK. However, for the legal and accounting professions, Scotland and Northern Ireland have different supervisory bodies that each have their own code of conduct. It is worth bearing in mind that such codes seek to bring members in compliance with the MLR 2017 and as a result are quite similar.

### 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

A number of supervisory authorities operating in the UK are required to ensure compliance with and enforcement of anti-money laundering requirements for organisations that fall within the scope of the MLR 2017 (see question 3.1 below).

When considering whether to commence criminal proceedings against a firm or an individual, a UK enforcement authority must apply the two limb test (known as the Full Code Test). The principles for the test are detailed in the Code for Crown Prosecutors, a publicly available document. When taking regulatory enforcement action, each authority has its own guidance that it will apply and is publicly available (see the FCA's Enforcement Guide).

### 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. As of October 2018, the National Economic Crime Centre (the **NECC**) began operating as the overarching body to coordinate the UK's response to economic crime, including money laundering. The NECC includes the Joint Money Laundering Intelligence Taskforce (**JMLIT**). JMLIT is a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats.

### 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). The FCA must bring enforcement proceedings within six years from the date it obtained information about the relevant misconduct.

### 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

supervisory authority may also apply to the court for an injunction where there has been or is a reasonable likelihood of a contravention of a relevant requirement.

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?**

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 including carrying out risk assessments, training and CDD). This is subject to a defence where the person took all reasonable steps and exercised all due diligence to avoid committing the offence.

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, where 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.

We are not aware of a financial institution challenging a money laundering penalty in the Upper 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 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, and tax advisers;
- independent legal professionals conducting transactional work;
- trust or company service providers;
- estate and letting agents;
- high value dealers, casinos, auction platforms, and art market participants; and
- cryptoasset exchange providers and custodian wallet providers.

The MLR 2017 impose requirements concerning risk assessments, ownership and control, AML policies and procedures, internal controls, training, recordkeeping, ongoing monitoring of business relationships, CDD, information on payer and payees (for payment service providers) and ceasing transactions in certain circumstances. Businesses are also compelled to provide information and/or documents to supervising authorities on request.

Additional obligations for financial institutions are contained within SYSC (located in the FCA Handbook), 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.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

Since 5MLD was brought into force via the MLR 2019 on 10 January 2020, cryptoasset exchange providers and custodian wallet providers have been brought within the scope of MLR 2017 and are now part of the "regulated sector".

**3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?**

Yes – the MLR 2017 (and, for financial institutions, the SYSC) impose requirements on the businesses listed at question 3.1 above to, where appropriate to the size and nature of its business, have effective AML systems and internal controls in place, including to assess compliance. Required elements include senior responsibility, employee screening, an independent internal audit function to monitor compliance and make recommendations, appointment of a nominated officer responsible for AML compliance, and timely internal reporting.

**3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?**

There are no specific requirements for recordkeeping or reporting large currency transactions. The general requirements regarding recordkeeping (set out in the MLR 2017 and SYSC as described above) and reporting (set out in POCA and the Terrorism Act 2000 as described above) would, however, apply to such transactions.

**3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.**

No. There are no specific AML requirements for financial institutions or other designated businesses in relation to routinely reporting large non-cash transactions.

**3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?**

No. There are no specific AML requirements for financial institutions or other designated businesses in relation to cross-border transactions reporting.

**3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?**

Financial institutions (and other firms in the regulated sector) in the UK are required to undertake customer identification and due diligence prior to establishing a business relationship with a customer. When entering a new business relationship with a customer, a firm must obtain information on:

- the customer's identity; and
- the purpose and intended nature of the business relationship (i.e. where funds will come from and the purpose of any contemplated transactions).

The type of information that a firm 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 are higher-risk money laundering situations which 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 identity of the customer or the customer's beneficial owner(s);
- applying extra measures to check documents supplied by a credit or financial institution; and
- understanding the source of funds and source of wealth of the customer and of the customer's beneficial owner.

5MLD has inserted enhanced due diligence measures for business relationships or transactions involving high-risk non-EEA countries.

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

Credit and financial institutions (as defined in the MLR 2017) are prohibited from entering into, or continuing, a correspondent relationship with a shell bank (MLR 2017 Regulation 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 Regulation 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.

**3.9 What is the criteria for reporting suspicious activity?**

The obligation to report suspicious activity pursuant to ss 330–332 POCA arises where a person concludes that they know, suspect or

have reasonable grounds to know or suspect that another person is or has engaged in a money laundering offence. Typically, the person discloses their suspicion to the firm's "nominated officer", the Money Laundering Reporting Officer (**MLRO**) who assesses and files Suspicious Activity Reports (**SAR**s) on the firm's (and their own) behalf. The MLRO will assess whether the reporting criteria is met and, if so, they are required to file a SAR. See question 1.2 for the criteria for a money laundering offence to be committed. The threshold for "suspicion" in this context is low. Suspicion has been defined in the POCA context as: "a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."

The mental test may be satisfied objectively (i.e. the reasonable person should suspect) or subjectively (i.e. the person does suspect).

Where a person (irrespective of whether they act in the regulated sector) considers they may be about to, are in the process of, or have already committed a money laundering offence, they may voluntarily decide to file a SAR in order to obtain a defence to the offence. This is known as an "authorised disclosure" with the disclosing party seeking "appropriate consent" to carry out a "prohibited act". Contrary to the term used in POCA, the NCA has come to refer to this as a DAML (Defence Against a Money Laundering offence). The regime more generally is known as the consent regime.

Once the SAR is submitted, a notice period begins for the NCA to consider its content and decide whether to take any enforcement action. This may include liaising with other enforcement authorities. The notice period is seven working days, beginning on the first working day after the SAR is submitted. If a person receives a DAML, they have consent to carry out the act. If they do not obtain a response from the NCA, as is increasingly common, within the seven-day notice period, they obtain "deemed consent" for the offence and, again, have a DAML. However, if a refusal notice is received within the seven-day period, a 31-day moratorium period begins starting from the day of the refusal. This period is intended to allow the NCA to disrupt the criminal activity by obtaining a POCA Restraint Order or, more typically since the CFA came into force, an Account Freezing Order. In practice, the authorities found it challenging to obtain a court order to freeze the funds within the moratorium period. Consequently, amendments were made to the consent regime via the CFA, which now provide the NCA with power to apply to court for an extension to the moratorium period. A court may grant an extension for a period of 31 days and may do so on more than one occasion, up to a maximum of 186 days.

All SARs are filed through the NCA's online portal.

### 3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?

There is a publicly accessible central government registry (Companies House) for UK company information on management and ownership. However, the ownership information may be up to a year out of date as non-listed companies are only required to provide this information to Companies House annually.

In practice, up-to-date share ownership information regarding shareholdings of 3%+ in a company with shares admitted to trading on a regulated or prescribed market is publicly available due to stringent notification requirements under the FCA's Disclosure Guidance and Transparency Rules. There is also a public register of Persons with Significant Control (**PSC**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 UK has registers of beneficial ownership for three different types of assets: companies; properties and land; and trusts. Information on the beneficial ownership of companies is publicly available without having to demonstrate legitimate interest. For properties owned by overseas companies and legal entities, the Government plans to launch a public beneficial ownership register in 2021. The register for trusts is not public.

The FATF report dated 1 December 2018 noted that the register was sometimes inaccurate, and there was no obligation on Companies House to update it at present when notified of inaccuracies. 5MLD, via the MLR 2019, has introduced a new "discrepancy reporting requirement" for obliged entities to alert Companies House to any discrepancy between beneficial ownership information on the People with Significant Control Register and any information made available to the firm during its own due diligence checks. Companies House may then investigate and remedy the discrepancy as required. An exception applies for Limited Liability Partnerships (**LLP**s).

The register does not, as of yet, extend to UK Crown Dependencies and Overseas Territories.

The Sanctions and Anti-Money Laundering Act 2018 (**SAMLA**) contains provisions on publicly accessible registers of company beneficial ownership in the UK Overseas Territories. Reasonable assistance must be provided to enable each of those governments to establish a publicly accessible register of the beneficial ownership of companies registered in each government's jurisdiction. The Secretary of State must, by 31 December 2020, prepare a draft Order in Council requiring the government of any British Overseas Territory that has not introduced a publicly accessible register of the beneficial ownership of companies within its jurisdiction to do so. At the date of this chapter, this provision is not yet in force.

### 3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?

Payment Service Providers (**PSP**s) must comply with requirements contained in the MLR 2017, derived from Chapter II, Section 1, Chapter 4 of the EU Funds Transfer Regulation. Complete payer and payee information (name, address, and account number) must generally accompany all wire transfers although there are limited exceptions. For example, if the Payment Service Providers of both payer and payee are located within the EU, then the wire transfer only need be accompanied by at least the account numbers of the payer and payee. Intermediary PSPs must ensure that all information received on the payer and payee which accompanies a wire transfer is retained with the transfer. Guidance provided by the JMLSG provides more detail on how to comply with these requirements and exceptions.

### 3.12 Is ownership of legal entities in the form of bearer shares permitted?

No. Bearer shares were abolished on 26 May 2015 when amendments to the UK Companies Act 2006 were implemented, via the Small Business, Enterprise and Employment Act 2015.

The changes were made as part of the UK Government's aim to promote transparency of company ownership and control in order to deter criminal misuse of companies in the UK. From 26 May 2015, UK companies were prohibited from issuing bearer shares, and companies with bearer shares in issue were required to take action to get rid of them.

### 3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Most of the UK money laundering offences described in question 1.2 apply to all businesses, subject to the jurisdictional requirements stated in question 1.3. However, only the businesses listed in question 3.1 (which include certain non-financial institution businesses) can commit the offences of "tipping-off" and "failure to disclose" under POCA.

The MLR 2017 apply to the businesses listed in question 3.1 above, which include certain non-financial institution businesses.

There are some specific requirements for PSPs. PSPs must comply with additional requirements contained in the MLR 2017, derived from the EU Funds Transfer Regulation. See question 3.11 above.

There are a very small number of sector-specific exceptions to the requirements in the MLR 2017; e.g., Regulation 31 (requirement to cease transactions) does not apply to certain professional advisers advising on the institution or avoidance of legal proceedings, and Regulation 32 contains a Customer Due Diligence exception for trustees of debt issues.

### 3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

By way of MLR 2019, operators of a "Freeport" which store art were brought within the scope of the AML requirements. Freeport means a warehouse or storage facility within an area designated by the Treasury as a special area for customs.

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.

The 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, or 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 or the MLR 2017. Some supervisory bodies have also produced guidance for members (e.g. the UK Law Society).

## 4 General

### 4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

On Brexit, the MLR 2017 were amended by the Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019 (2019 No. 253), to reflect the fact that the UK is no longer an EU Member State. The main changes are:

- The equalisation of due diligence requirements applied to intra-EEA correspondent banking relationships (to bring them in line with non-EEA banks).
- The European Commission's high-risk third country list will be "on shored" (i.e. become part of UK law as at a particular date) but will not be dynamic, i.e. will not track changes at EU level; the list will only evolve as amended by UK law.
- New powers for the FCA to make technical standards to specify what additional measures are required to be taken by credit and financial institutions with branches or subsidiaries abroad. This function is currently exercised by the European Commission.
- The equalisation of information requirements for fund transfers both in and outside the EU. The effect of this will be to require UK PSPs to provide greater volumes of information accompanying transfers of funds into EU Member States than is currently the case.
- The removal of mandatory regard to guidelines published by the European Supervisory Authorities (although they are still likely to be taken into account by the FCA).
- Removal of need for transmission of information (such as the UK's National Risk Assessments of Money Laundering and Terrorist Financing) to EU institutions and other Member States.

These regulations will come into force at the end of the transition period, currently forecast for 31 December 2020.

The Sixth EU Money Laundering Directive (**6MLD**) came into force on 2 December 2018, with Member States required to implement it by 3 December 2020. However, the UK has opted out of 6MLD on the basis that it considers itself "already largely compliant with the Directive". Nevertheless, 6MLD introduces an offence akin to a "failure to prevent" money laundering offence which is not currently within the scope of English law, but which has been raised for introduction in UK Government and Law Commission consultations within the last three years. It will therefore be interesting to monitor whether the UK adopts similar legislation in line with the EU and/or as part of a wider introduction of a corporate "failure to prevent" economic crime offence.

SAMLA enables the government to implement sanctions and to amend or replace the MLR 2017 and implement the FATF standards once the UK is no longer bound by EU law. The UK has not indicated that it wishes to amend the AML regime in any meaningful way post Brexit.

One aspect of the AML regime that is under consideration for reform is the "consent regime" (referred to in question 3.9 above). In 2017, the Home Office tasked the Law Commission to assess whether there was scope to reform this voluntary disclosure regime. It conducted a wide-ranging consultation process involving stakeholders in the public and private sector. In June 2019, it published its report containing 19 recommendations. A response is awaited from the Home Office. The recommendations (if adopted) would not amount to wholesale reform of the AML regime. Principally the report recommended:

- retaining the consent regime, subject to amendments to improve effectiveness; and
- the creation of statutory guidance on a number of key legislative concepts underpinning the reporting regime, to assist the regulated sector in complying with their legal obligations. This includes guidance on suspicion, appropriate consent and arrangements with prior consent, and what may amount to a reasonable excuse.

**4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?**

The Report on the Fourth Round Mutual Evaluation of the UK by the FATF dated 1 December 2018 concluded that: "[t]he UK has implemented an AML/CTF system that is effective in many respects. Particularly good results are being achieved in the areas of investigation and prosecution of ML/TF, confiscation, the implementation of targeted financial sanctions related to terrorism and proliferation, protecting the non-profit sector from terrorist abuse, understanding the ML/TF risks facing the country, preventing misuse of legal structures and co-operating domestically and internationally to address them. However, major improvements are needed to strengthen supervision and implementation of preventive measures, and ensure that financial intelligence is fully exploited."

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The Report on the Fourth Round Mutual Evaluation of the UK by the FATF was published on 1 December 2018. The IMF conducted a Financial Sector Assessment Programme for the UK in the areas of AML/CTF. Its report was published in June 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 (http://www.fca.org.uk).

The UK Parliament website contains the relevant Acts of Parliament, secondary legislation and information on parliamentary debates, committee reports and proposed new laws (http://www.parliament.uk).

**John Gibson** is a partner in the London office of Cohen & Gresser. He leads the firm's United Kingdom white collar and investigations practice. John's work focuses on complex economic crime, investigations, and regulatory matters. He draws on over two decades of litigation and advisory experience, first as a trial lawyer in independent practice and then, for five years, as one of the most senior prosecutors and investigation managers in the Bribery & Corruption Unit of the UK's Serious Fraud Office (**SFO**).

**Cohen & Gresser (UK) LLP**
2–4 King Street
London, SW1Y 6QP
United Kingdom

Tel: +44 20 8037 2324
Email: jgibson@cohengresser.com
URL: www.cohengresser.com

**Tim Harris** is an associate in Cohen & Gresser's London office. His practice focuses on white collar criminal defence, including internal and regulatory investigations. Tim has represented a wide range of companies and individuals in complex financial crime and regulatory matters. During his career, he has been involved in a number of London's highest-profile investigations, trials, and public inquiries. Tim also provides non-contentious advice with respect to tax evasion, anti-bribery and corruption, and anti-money laundering regulations.

**Cohen & Gresser (UK) LLP**
2–4 King Street
London, SW1Y 6QP
United Kingdom

Tel: +44 20 8036 9395
Email: tharris@cohengresser.com
URL: www.cohengresser.com

Cohen & Gresser is an international law firm with offices in New York, Seoul, Paris, Washington, D.C., and London. We have an outstanding record of success in high-stakes and high-profile litigation, investigations, and transactional work for our clients, including major financial institutions and companies across the world. Our attorneys have superb credentials, and are committed to providing the efficiency and personal service of a boutique law firm along with the quality and attention to detail that are the hallmarks of the best firms in the world. The firm has been recognised in a wide range of publications, including *Chambers*, *The Legal 500*, *Global Investigations Review*, *Managing IP*, *U.S. News & World Report*'s "Best Law Firms", *Décideurs*, and *Benchmark Litigation*. We have also been named to *The National Law Journal*'s "Midsize Hot List" and the BTI *Client Service A-Team*, and over half of our U.S.-based attorneys have been recognised by *Super Lawyers*.

**www.cohengresser.com**

COHEN & GRESSER (UK) LLP

# USA


Joel M. Cohen

Linda Noonan

Gibson, Dunn & Crutcher LLP


## 1 The Crime of Money Laundering and Criminal Enforcement

### 1.1 What is the legal authority to prosecute money laundering at the national level?

Money laundering has been a crime in the United States since 1986, making the United States one of the first countries to criminalise money laundering conduct. There are two money laundering criminal provisions, 18 United States Code, Sections 1956 and 1957 (18 U.S.C. §§ 1956 and 1957).

### 1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Generally, it is a crime to engage in virtually any type of financial transaction if a person conducted the transaction with knowledge that the funds were the proceeds of "criminal activity" and if the government can prove the proceeds were derived from a "specified unlawful activity." Criminal activity can be a violation of any criminal law – federal, state, local, or foreign. Specified unlawful activities are set forth in the statute and include over 200 types of U.S. crimes, from drug trafficking, terrorism, and fraud, to crimes traditionally associated with organised crime, and certain foreign crimes, as discussed below in question 1.3.

The government does not need to prove that the person conducting the money laundering transaction knew that the proceeds were from a specified form of illegal activity.

Knowledge can be based on wilful blindness or conscious indifference – failure to inquire when faced with red flags for illegal activity. Additionally, knowledge can be based on a government "sting" or subterfuge where government agents represent that funds are the proceeds of illegal activity.

Under Section 1956, the transaction can be: (1) with the intent to promote the carrying on of the specified unlawful activity; (2) with the intent to engage in U.S. tax evasion or to file a false tax return; (3) knowing the transaction is in whole or in part to disguise the nature, location, source, ownership or control of the proceeds of a specified unlawful activity; or (4) with the intent to avoid a transaction reporting requirement under federal or state law.

Section 1956 also criminalises the transportation or transmission of funds or monetary instruments (cash or negotiable instruments or securities in bearer form): (1) with the intent to promote the carrying out of a specific unlawful activity; or (2) knowing the funds or monetary instruments represent the proceeds of a specified unlawful activity and the transmission or transportation is designed in whole or in part to conceal or disguise the nature, location, source, ownership or control of the proceeds of the specified unlawful activity.

Under Section 1957, it is a crime to knowingly engage in a financial transaction in property derived from specified unlawful activity through a U.S. bank or other "financial institution" or a foreign bank (in an amount greater than $10,000). Financial institution is broadly defined with reference to the Bank Secrecy Act ("BSA") statutory definition of financial institution (31 U.S.C. § 5312(a)(2)) and includes not just banks, but a wide range of other financial businesses, including securities broker-dealers, insurance companies, non-bank finance companies, and casinos.

Tax evasion is not itself a predicate offence, but, as noted, conducting a transaction with the proceeds of another specified unlawful activity with the intent to evade federal tax or file a false tax return is subject to prosecution under Section 1956. Also, wire fraud (18 U.S.C. § 1343) is a specified unlawful activity. Wire fraud to promote tax evasion, even foreign tax evasion, can be a money laundering predicate offence. *See Pasquantino v. U.S.*, 544 U.S. 349 (2005) (wire fraud to defraud a foreign government of tax revenue can be a basis for money laundering).

### 1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

There is extensive extraterritorial jurisdiction under the money laundering criminal provisions. Under Section 1956, there is extraterritorial jurisdiction over money laundering conduct (over $10,000) by a U.S. citizen anywhere in the world or over a non-U.S. citizen if the conduct occurs at least "in part" in the United States. "In part" can be a funds transfer to a U.S. bank.

Under Section 1957, there is jurisdiction over offences that take place outside the United States by U.S. persons (citizens, residents, and legal persons) and by non-U.S. persons as long as the transaction occurs in whole or in part in the United States.

Certain foreign crimes are specified unlawful activities, including drug crimes, murder for hire, arson, foreign public corruption, foreign bank fraud, arms smuggling, human trafficking, and any crime subject to a multilateral extradition treaty with the United States.

Generally, there is no extraterritorial jurisdiction under the BSA, discussed below in section 2. The BSA requirements for Money Services Businesses ("MSBs") can apply, however, even if the MSB has no physical presence in the United States if the business conducts business "wholly or in substantial part within the United States," *i.e.*, if a substantial number of U.S. customers or recipients of funds transfers are in the United States. 31 C.F.R. § 1010.100(ff) (BSA definition of MSB).

### 1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

Prosecution of money laundering crimes is the responsibility of the U.S. Department of Justice. There is a special unit in the Criminal Division of the Department of Justice, the Money Laundering and Asset Recovery Section ("MLARS"), that is responsible for money laundering prosecution and related forfeiture actions. The 94 U.S. Attorney's Offices across the United States and its territories also may prosecute the crime of money laundering alone or with MLARS. MLARS must approve any prosecution of a financial institution by a U.S. Attorney's Office.

As required in Section 1956(e), there is a (non-public) memorandum of understanding among the Secretary of the Treasury, the Secretary of Homeland Security, the Attorney General, and the Postal Service setting forth investigative responsibilities of the various federal law enforcement agencies that have investigative jurisdiction over Sections 1956 and 1957. Jurisdiction is generally along the lines of the responsibility for the investigation of 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 of up to $500,000 or double the amount of property involved, whichever is greater, for each violation, and for individuals, imprisonment of up to 20 years for each violation.

### 1.7 What is the statute of limitations for money laundering crimes?

That statute of limitations is five years. 18 U.S.C. § 3282(a).

### 1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Section 1956(d) specifically provides that it does not supersede any provisions in federal, state or other local laws imposing additional criminal or civil (administrative) penalties.

Many states, including New York and California, have parallel money laundering criminal provisions under state law. *See, e.g.*, New York Penal Law Article 470.

### 1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

There is both criminal forfeiture following a conviction for money laundering, and civil forfeiture against the assets involved in, or traceable to, money laundering criminal conduct.

Under 18 U.S.C. § 982, if a person has been convicted of money laundering, any property, real or personal, involved in the offence, or any property traceable to the offence, is subject to forfeiture.

Under 18 U.S.C. § 981, a civil forfeiture action can be brought against property involved in or is traceable to the money laundering conduct even if no one has been convicted of money laundering. Because this is a civil action, the standard of proof for the government is lower than if there were a criminal prosecution for the money laundering conduct (preponderance of the evidence versus beyond a reasonable doubt). There is no need to establish that the person alleged to have committed money laundering is dead or otherwise unavailable.

### 1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Absent established collusion with money launderers or other criminals, very few directors, officers, or employees have been convicted of money laundering. Where there have been criminal settlements with banks and other financial institutions related to money laundering, in all but two cases, the settlements have been based on alleged violations of the Bank Secrecy Act ("BSA"), not violations of the money laundering criminal offenses.

### 1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Since 2002, 35 regulated financial institutions (26 banks) have pled guilty or have reached settlements with the Department of Justice, generally, as noted, based on alleged violations of the anti-money laundering regulatory requirements under the BSA (either failure to maintain an adequate anti-money laundering program and/or failure to file required Suspicious Activity Reports).

A few of these settlements with foreign-owned banks have been based on alleged sanctions violations in addition to BSA violations. Substantial fines or forfeitures were paid as part of these settlements. There also were two other BSA prosecutions of banks in the late 1980s relating to currency transaction reporting and the Bank of Credit and Commerce International ("BCCI") pled guilty to money laundering in 1990.

In connection with many of the criminal dispositions, civil (administrative) sanctions based on the same or related misconduct have been imposed at the same time by federal and/or state regulators and the Department of the Treasury 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 charter or federal deposit insurance, *i.e.*, be forced to cease operations. Such a review is discretionary if a bank is convicted of BSA violations and, in practice, not conducted. *See, e.g.*, 12 U.S.C. § 1818(w) (process for state-licensed, federally-insured banks).

Records relating to the criminal settlements are publicly available, including, in most cases, lengthy statements by the government about underlying facts that led to the criminal disposition. To our knowledge, there have been no non-public criminal settlements with financial institutions.

## 2 Anti-Money Laundering Regulatory/ Administrative Requirements and Enforcement

### 2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

**Authorities**

In the United States, the main anti-money laundering ("AML") legal authority is the Bank Secrecy Act, 31 U.S.C. § 5311 *et seq.*, 12 U.S.C. §§ 1829b and 1951–1959 (the "BSA statute"), and the Bank Secrecy Act implementing regulations, 31 C.F.R. Chapter X (the "BSA regulations"). (The BSA statute and regulations collectively will be referred to as "the BSA.") The BSA statute was originally enacted in 1970 and has been amended several times, including significantly in 2001 by the USA PATRIOT Act ("PATRIOT Act"). The BSA gives the Secretary of the Treasury the authority to implement reporting, recordkeeping, and anti-money laundering program requirements by regulation for financial institutions and other businesses listed in the statute. 31 U.S.C. § 5312(a)(2). The Secretary of the Treasury has delegated the authority to administer and enforce the BSA to a Department of the Treasury bureau, FinCEN. FinCEN also is the U.S. Financial Intelligence Unit. *See* question 2.6. Because FinCEN has no examination staff, it has further delegated BSA examination authority for various categories of financial institutions to their federal functional regulators (federal bank, securities, and futures regulators). Examination authorities for financial institutions and businesses without a federal functional regulator is discussed in question 2.5.

The federal banking regulators (the Office of the Comptroller of the Currency (the "OCC"), the Board of Governors of the Federal Reserve ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA")) have parallel regulatory authority to require BSA compliance programs and suspicious activity reporting for the institutions for which they are responsible. *See, e.g.*, 12 C.F.R. §§ 21.21 (OCC BSA program requirement), 21.12 (OCC suspicious activity reporting requirement). Consequently, the bank regulators have both delegated examination authority from FinCEN, as federal functional regulators, and independent regulatory enforcement authority.

BSA examination authority for broker-dealers has been delegated to the Securities and Exchange Commission ("SEC"), as the federal functional regulator for broker-dealers. The SEC has further delegated authority to the Financial Industry Regulatory Authority ("FINRA"), the self-regulatory organization ("SRO") for broker-dealers. The SEC also has incorporated compliance with the BSA requirements for broker-dealers into SEC regulations and, consequently, has independent authority to enforce the BSA. 17 C.F.R. §§ 240.17a-8, 405.4.

Similarly, BSA examination authority for futures commission merchants ("FCMs") and introducing brokers in commodities ("IB-Cs"), which are financial institutions under the BSA, has been delegated by FinCEN to the Commodities Futures Trading Commission ("CFTC"), as their federal functional regulator. The CFTC also has incorporated BSA compliance in its regulations. 17 C.F.R. § 42.2. The CFTC has delegated authority to the National Futures Authority ("NFA") as that industry's SRO.

**AML Requirements**

For the United States, the response to the question of what requirements apply is complicated. The BSA statute generally is not self-executing and must be implemented by regulation. The scope and details of regulatory requirements for each category of financial institutions and financial businesses subject to BSA vary. To further complicate the issue, all these businesses are defined as financial institutions under the BSA statute, but only certain ones are designated as financial institutions under the BSA regulations, *i.e.*, banks, broker-dealers, FCMs, IB-Cs, mutual funds, MSBs, casinos, and card clubs. Some BSA requirements only apply to businesses that come within the BSA regulatory definition of financial institution.

There also are three BSA requirements that apply to all persons subject to U.S. jurisdiction or to all U.S. trades businesses, not just to financial institutions or other businesses subject to specific BSA regulatory requirements. *See* question 3.13.

**Main Requirements**

These are the main requirements that apply under the BSA regulations, most of which are discussed in more detail in Part 3, as cross-referenced below.

- **AML Programs**: All financial institutions and financial businesses subject to the BSA regulations are required to maintain risk-based AML Programs with certain minimum requirements to guard against money laundering. *See* questions 3.1, 3.2 and 3.3.
- **Currency Transaction Reporting**: "Financial institutions," as defined under the BSA regulations, must file Currency Transaction Reports ("CTRs"). *See* question 3.4.
- **Cash Reporting or Form 8300 Reporting**: This requirement applies to all other businesses that are subject to the AML Program requirement, but not defined as financial institutions under the BSA regulations, and all other U.S. trades and businesses. *See* questions 3.4 and 3.13.
- **Suspicious Transaction Reporting**: Financial institutions and other businesses subject to the AML Program requirement (except Check Cashers, Operators of Credit Card Systems, and Dealers in Precious Metals, Precious Stones, or Jewels) must file Suspicious Activity Reports ("SARs"). *See* question 3.9.
- **Customer Due Diligence ("CDD") Programs**: Banks, broker-dealers, FCMs, IB-Cs, and mutual funds are required to maintain CDD programs as part of their AML programs. *See* question 3.7.
- **Customer Identification Program ("CIP")**: Certain BSA financial institutions (banks, broker-dealers, FCMs, IB-Cs, and mutual funds) are required to maintain CIP programs as part of their CDD and AML Programs. *See* question 3.7.
- **Customer Due Diligence Programs for Non-U.S. Private Banking Clients and Foreign Correspondents**: This requirement is applicable to banks, broker-dealers, FCMs, IB-Cs, and mutual funds. *See* question 3.7.

- **Recordkeeping**: There are BSA general recordkeeping requirements applicable to all BSA financial institutions, specific recordkeeping requirements for specific types of BSA financial institutions, and requirements to maintain records related to BSA compliance for all financial institutions and financial businesses subject to the BSA. Generally, records are required to be maintained for five years. 31 C.F.R. § 1010.410 (general recordkeeping requirements for financial institutions); *see, e.g.*, 31 C.F.R. § 1023.410 (recordkeeping requirements for broker-dealers).
- **Cash Sale of Monetary Instruments**: There are special recordkeeping and identification requirements relating to the cash sale of monetary instruments in amounts of $3,000 to $10,000 inclusive (bank checks or drafts, cashier's checks, travellers' cheques, and money orders) by banks and other financial institutions under the BSA regulations. 31 C.F.R. § 1010.415.
- **Funds Transfer Recordkeeping and the Travel Rule**: This is applicable to banks and other financial institutions under the BSA regulations. *See* question 3.11.
- **Money Services Business Registration**: MSBs must register (and re-register every two years) with FinCEN. MSBs that are only MSBs because they are agents of another MSB are not required to register. MSBs must maintain lists of their agents with certain information and provide the lists to FinCEN upon request. Sellers of prepaid access (unless MSBs by virtue of other business activities) are excepted from registration. 31 C.F.R. § 1022.380.
- **Government Information Sharing or Section 314(a) Sharing**: Periodically and on an *ad hoc* basis, banks, broker-dealers, and certain large MSBs receive lists from FinCEN of persons suspected of terrorist activity or money laundering by law enforcement agencies. The financial institutions must respond with information about accounts maintained for the persons and certain transactions conducted by them in accordance with guidance from FinCEN that is not public. The request and response are sent and received via a secure network. Strict confidentiality is required about the process. 31 C.F.R. § 1010.520.
- **Voluntary Financial Institution Information Sharing or Section 314(b) Sharing**: Financial institutions or other businesses required to maintain AML Programs under the BSA regulations may voluntarily register with FinCEN to participate in sharing information with each other. The request can only be made for the purpose of identifying and/or reporting activity that the requestor suspects may be involved in terrorist activity or money laundering. The information received may only be used for SAR filing, to determine whether to open or maintain an account or conduct a transaction, or for use in BSA compliance. Strict confidentiality about the process must be maintained by participants. If all requirements are satisfied, there is a safe harbour from civil liability based on the disclosure. 31 C.F.R. § 1010.540.
- **Section 311 Special Measures**: Under Section 311 of the PATRIOT Act, FinCEN can impose a range of special measures against a foreign jurisdiction or foreign financial institution that is designated as posing primary money laundering concern. One of the measures frequently imposed is to prohibit U.S.-covered financial institutions (banks, broker-dealers, FCMs, IB-Cs, and mutual funds) from providing correspondent accounts directly or indirectly to the financial institutions subject to special measures and to notify their correspondent accountholders that they cannot offer services to the designated financial institutions through their correspondent account with the U.S. institution.

### 2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

As discussed in question 2.1, the SROs for the securities and futures industries have imposed requirements on their members that are subject to the BSA 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, with approval of the CFTC, the NFA has issued AML Program requirements, under NFA Compliance Rule 2-9(c) for FCMs and IB-Cs. *See* question 2.1.

### 2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

FINRA examines broker-dealers for compliance with AML Program requirements and, more frequently than any regulatory agency, brings enforcement actions against its members, which can include civil penalties against firms and individual officers and employees (including AML compliance officers), compliance undertakings, and in some cases, termination of firms and suspension or revocation of licences of officers and employees. The NFA also has brought similar enforcement actions based on examinations of FCMs and IB-Cs.

### 2.4 Are there requirements only at national level?

Many states impose parallel requirements on state-licensed financial institutions, *e.g.*, state-licensed banks and money services businesses, such as check cashers and money transmitters. Coverage and requirements vary by state.

The New York Department of Financial Services ("DFS") is the most active state regulator in AML and sanctions enforcement. In some recent cases, it has brought enforcement actions with large civil monetary penalties against New York branches and subsidiaries of foreign banks even where no federal regulator has imposed a penalty. The actions are based on the banks' failures to maintain books and records under New York law relating to their alleged BSA and sanctions failures. New York Banking Law §§ 39 (books and records provision) and 44 (penalty provisions). In connection with one enforcement action, DFS also required a foreign bank to surrender the license of its branch to do business in New York.

New York also requires suspicious activity reporting by New York-licensed financial institutions, which has been interpreted to include reporting of potential money laundering activity. 3 N.Y.C.R.R. Part 300.

New York has implemented a unique requirement in Part 504 of the Banking Superintendent's Regulations, which is applicable to New York-licensed banks, check cashers, and money transmitters. Part 504 requires annual compliance statements, *i.e.*, certifications, by a resolution of the Board of Directors or a "compliance finding" by a senior officer confirming that: (1) the financial institution maintains a risk-based transaction monitoring system to identify potential suspicious activity for purposes of compliance with the BSA suspicious activity reporting requirement (and a risk-based sanctions filtering system to comply with sanctions requirements); and (2) certain facts relating to the maintenance, design, and implementation of those systems. The first annual board resolution or senior officer compliance finding under Rule 504 was due on April 15, 2018. NYDFS Superintendent's Regulations § 504.1-6.

### 2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? If so, are the criteria for examination publicly available?

**Responsible Authorities**

As discussed in question 2.1, FinCEN does not have examination staff and has delegated an examination authority to the federal functional regulators for the financial institutions for which they are responsible. The federal functional regulators are: the OCC; Federal Reserve; FDIC; NCUA; SEC (broker-dealers and mutual funds); and CFTC (FCMs and IB-Cs). The SEC and CFTC retain authority, but also have delegated authority to the SROs, FINRA and NFA.

Examination responsibility for the housing government-sponsored enterprises (the Federal Home Loan Mortgage Corporation ("Freddie Mac") and the Federal National Mortgage Association ("Fannie Mae")) is with the Federal Housing Finance Agency, the conservator for these entities.

For all other financial institutions and businesses subject to AML Program requirements, the examination authority has been delegated to the Internal Revenue Service ("IRS"). This includes money services businesses, casinos, card clubs, insurance companies (with respect to certain products), dealers in precious metals, precious stones, and jewels, operators of credit card systems and non-bank residential mortgage originators and lenders.

FinCEN has entered a number of agreements with state insurance commissioners providing for BSA examinations of insurance companies by state insurance examiners.

**Examination Criteria**

The most useful public guidance is the *Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual* for banks ("FFIEC Manual"), available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

This manual was originally compiled by FinCEN and other federal banking agencies in 2006 and, with the exception of two chapters (the CDD chapter and a new chapter on beneficial ownership) updated in 2018, was last updated in 2014. A comprehensive update is expected to be issued in segments over the course of 2020.

There is no analogous published examination guidance for the securities industry.

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.

The IRS Manual provides information on BSA "examination techniques" for BSA examination for the sectors for which IRS has examination responsibility. This is available at https://www.irs.gov/irm/part4/irm_04-026-009#idm140691809929120.

### 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.

FinCEN, the federal functional regulators, and the SROs also can impose monetary penalties on directors, officers and employees. 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.

In March 2020, FinCEN imposed a civil money penalty, based on BSA violations, against the former Chief Risk Officer of a major American bank.

**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. A party could challenge the terms of enforcement in a judicial action, but that happens rarely because financial institutions generally conclude settlements with relevant authorities.

## 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.
- CDD Program requirements.

Certain requirements only apply to those within the BSA definition of financial institution, *i.e.*, banks, broker-dealers, FCMs, IB-Cs, mutual funds, MSBs, casinos, and card clubs:

- CTR reporting.
- Funds transfer recordkeeping and the Travel Rule.
- Recordkeeping for cash sales of monetary instruments.

Companies that offer new payment technologies or alternative currencies may be subject to BSA requirements as MSBs, including the requirement to register with FinCEN, if their activities come under the definition of MSB as a money transmitter or provider of prepaid access. These companies can apply to FinCEN for an administrative ruling to determine their status under the BSA if it is not clear under the regulations. As discussed in question 3.2, FinCEN considers administrators and exchangers of virtual currency to be MSBs.

Currently, investment funds other than mutual funds are not subject to AML requirements. There are pending BSA regulations that will require SEC-registered investment advisers to maintain AML 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. It is not clear whether the proposal will be finalized. 80 Federal Register 52680 (Sept. 1, 2015).

Non-bank finance companies, other than residential mortgage lenders and originators, are not subject to BSA regulatory requirements, although the BSA statute provides authority to apply BSA requirements to a loan or finance company or pawnbroker.

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 3.14 below, on a temporary basis, title insurance companies in nine U.S. metropolitan areas have been subject to certain reporting requirements. FinCEN also encourages real estate agents, escrow agents, title companies, and others involved in real estate transactions to file SARs voluntarily.

**3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?**

In 2013, FinCEN issued guidance that administrators and exchangers of virtual currency are money transmitters under the BSA and consequently, are subject to the BSA MSB requirements for AML programs, suspicious activity reporting, and FinCEN registration. FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/sites/default/

files/shared/FIN-2013-G001.pdf. Further guidance was issued in 2019 clarifying FinCEN's position on which virtual currency business models will be subject to the BSA. FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual.

In February 2020, the Secretary of the Treasury stated publicly that additional AML requirements will be imposed on the virtual currency industry.

### 3.3 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

All the financial institutions and financial businesses subject to the BSA (listed in question 3.1) are required to maintain risk-based AML Programs to guard against money laundering with four minimum requirements, sometimes referred to as the four pillars of a program: (1) policies, procedures and internal controls; (2) designation of a compliance officer; (3) training; and (4) periodic independent testing of the program. For financial institutions subject to the CIP requirements (banks, broker-dealers, FCMs and IB-Cs, and mutual funds), the financial institution's CIP must be part of the AML Program. Similarly, for these same financial institutions, new CDD Program requirements and due diligence programs under Section 312 must be part of their AML Programs.

There is a regulatory expectation that the program be executed in accordance with a formal risk assessment. As noted, the authority for specific program requirements may be found in the BSA regulations, the regulations of the federal functional regulator or a rule of the SRO. 31 U.S.C. § 5318(h) (statutory requirement for AML Programs); *see, e.g.*, 31 C.F.R. § 1022.210 (AML Program requirements for MSBs).

### 3.4 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

**Currency Transaction Reporting**

Financial institutions (defined as financial institutions under the BSA regulations) must file CTRs with FinCEN on all transactions in (physical) currency in excess of $10,000 (or the foreign equivalent) conducted by, through, or to the financial institution, by or on behalf of the same person, on the same day. 31 C.F.R. § 1010.310–315.

It is prohibited to "structure" transactions to cause a financial institution not to file a CTR or to file an inaccurate CTR by breaking down transactions into smaller amounts at one or more financial institutions over one or more days. 31 C.F.R. § 1010.314.

Banks (and only banks) may exempt the transactions of certain customers from CTR reporting if BSA requirements relating to exemptions are followed. 31 C.F.R. § 1020.315.

**Cash Reporting or Form 8300 Reporting**

Other businesses subject to the AML Program requirements, but not defined as financial institutions under the BSA regulations, are subject to the requirement to report on cash *received* in excess of $10,000 (or the foreign equivalent) by the same person on the same day or in one or a series of related transactions on one or more days. Under some circumstances, cash can include cash-equivalent monetary instruments (bank cheques or drafts, cashier's cheques, money orders, and travellers' cheques) for reporting purposes. Insurance companies, operators of credit card systems, dealers in precious metals, precious stones, or jewels, non-bank mortgage lenders and originators, and housing government-sponsored enterprises are subject to Form 8300 reporting, and not to CTR reporting, to the extent they receive currency.

Under the BSA and parallel requirements under the Internal Revenue Code, the same cash reporting requirements apply to all trades or businesses in the United States without respect to whether other BSA requirements apply to them. 31 C.F.R. § 1010.330.

### 3.5 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

No, with the exception of requirements imposed on a temporary basis under BSA Geographic Targeting Orders. *See* question 3.14.

### 3.6 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

With some exceptions for financial institutions, all persons who transport, mail, or ship (or cause to be transported, mailed, or shipped) currency and/or other "monetary instruments" into or out of the United States in the amount of $10,000 or more (or the foreign equivalent) must file a Currency and Other Monetary Instrument Report ("CMIR") with U.S. Customs and Border Protection.

Monetary instruments in this context include travellers' cheques in any form, checks signed with the payee name blank, negotiable instruments, and securities in bearer form, in addition to currency. 31 C.F.R. §§ 1010.340 (CMIR requirement), 1010.100(dd) (definition of monetary instrument).

### 3.7 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

**Customer Due Diligence**

Pursuant to regulatory requirements, which became effective May 11, 2018, as part of their AML Programmes, certain financial institutions (banks, broker-dealers, mutual funds, FCMs and IB-Cs) must implement formal risk-based CDD programs that include certain minimum elements, including customer identification and verification (under a Customer Identification Program), obtaining information about the nature and purpose of a customer's account, ongoing monitoring of customer accounts, obtaining beneficial ownership information at a 25% threshold for legal entity customers and identifying a control person for legal entity customers (with certain exceptions). *See, e.g.*, 31 C.F.R. § 1020.210 (AML Program requirements for banks); 31 C.F.R. § 1010.230 (beneficial ownership requirements).

There also is a specific BSA requirement to maintain CDD programs for non-U.S. persons' private banking accounts and foreign correspondent accounts. The same covered financial institutions as for CDD programs (banks, broker-dealers, mutual funds, FCMs and IB-Cs) must maintain a CDD program for non-U.S. private banking accounts established on behalf of, or

for the benefit of, a non-U.S. person and foreign correspondent customers and an enhanced due diligence ("EDD") program for those relationships posing a higher risk. These programs must be designed to detect and report suspicious activity with certain minimum standards. These requirements are based on Section 312 of the PATRIOT Act and are often referred to as Section 312 requirements. 31 C.F.R. §§ 1010.610 (due diligence for foreign correspondent accounts), 1010.620 (due diligence for private banking for non-U.S. persons).

Even before the new CDD requirements, for many years, FinCEN and the federal functional regulators expected risk-based CDD to be a core component of AML Programs, with EDD expected for higher risk customers. The FFIEC Manual is a useful reference for which customers should be considered higher risk, *e.g.*, MSBs, non-government organisations, and Politically-Exposed Persons ("PEPs").

**Customer Identification Program**

The same financial institutions subject to the CDD requirements, (banks, broker-dealers, mutual funds, and FCMs and IB-Cs) are required to maintain CIPs setting forth how they will comply with the CIP regulatory requirements. The CIP regulations require financial institutions to obtain and record basic identification information (name, street address, date of birth, and identification number for an individual), and verify the identity of the customer through reliable documentary or non-documentary means. *See, e.g.*, 31 C.F.R. § 1020.220 (CIP requirements for banks).

**3.8 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?**

Banks, broker-dealers, mutual funds, FCMs and IB-Cs are prohibited from establishing, maintaining, administering, or managing accounts for foreign shell banks, which are entities effectively unregulated by any prudential supervisor. Shell banks are banks with offshore licences and no physical presence in the country where they are licensed (no offices, employees, or records). Shell banks do not include affiliates of regulated financial institutions (banks that have physical locations and are regulated by a supervisor in the licensing jurisdiction) with offshore licences. 31 C.F.R. § 1010.630.

**3.9 What is the criteria for reporting suspicious activity?**

Financial institutions and other businesses subject to the AML Program requirement (except Check Cashers, Operators of Credit Card Systems, and Dealers in Precious Metals, Precious Stones, or Jewels) are required to file SARs with FinCEN under the BSA (and for banks, under parallel requirements of their federal functional regulators). SARs are required where the filer "knows, suspects, or has reason to suspect" a transaction conducted or attempted by, at or through the financial institution: (1) involves money laundering; (2) is designed to evade any BSA regulation or requirement; (3) has no business or apparent lawful purpose or is not the sort in which a particular customer would engage; or (4) involves the use of the financial institution to facilitate criminal activity or involves any known or suspected violation of federal criminal law. *See, e.g.*, 31 C.F.R. § 1023.320(c) (SAR requirements for broker-dealers).

Generally, the reporting threshold is $5,000 or more. For banks, if the suspect is unknown, it is $25,000 or more. For MSBs, generally, it is $2,000 or more.

There are very few exceptions to the SAR requirements. For instance, securities broker-dealers and FCMs and IB-Cs are not required to file SARs on violations of securities or future laws by their employees unless they otherwise involve BSA violations, if the information is filed with the SEC, CFTC or their SRO. *See, e.g.*, 31 C.F.R. § 1023.330 (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 U.S.C. § 5318(g)(3); *see, e.g.* 31 C.F.R. § 1020.320(f) (safe harbour for banks). There is no safe harbour from criminal liability. If a financial institution identified potential suspicious activity, it must decide whether to terminate the customer relationship if further dealing could lead to liability for money laundering. With very rare exceptions, regulators will not direct a financial institution to terminate a customer relationship.

Generally, there is no requirement to notify any government agency that a SAR is being filed. However, FinCEN has issued guidance recommending that prior to closing an account when the financial institution is aware of an ongoing government investigation of the customer, there should be notification to the investigating agency. The agency may request that the financial institution retain the relationship for a period of time to facilitate the investigation.

**3.10 Does the government maintain current and adequate information about legal entities and their management and ownership, i.e., corporate registries to assist financial institutions with their anti-money laundering customer due diligence responsibilities, including obtaining current beneficial ownership information about legal entity customers?**

The requirements vary by state. In many, if not most states, the answer is no. Federal legislation to rectify the situation has been proposed several times, but has not been enacted mainly because of the cost and complexity of building a reliable corporate registry with accurate and current ownership information and harmonising state practices.

On October 22, 2019, the U.S. House of Representatives passed legislation (H.R. 2513 – The Corporate Transparency Act of 2019) that would establish a corporate registry with beneficial ownership information for corporations and limited liability companies (with exceptions) at FinCEN. A parallel bill is pending in the U.S. Senate (S. 2563 – the ILLICIT CASH Act).

**3.11 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions?**

Banks and other financial institutions under the BSA must maintain accurate records relating to funds transfers of $3,000 or more originated by customers and non-customers and verify the identity of non-customers originating funds transfers. The information required to be maintained depends on the role of the financial institution in the payment chain, *i.e.*, originator,

intermediary, or beneficiary institution. Financial institutions acting as originator or intermediary financial institutions must cause the information to "travel" to the next financial institution under the BSA Travel Rule. 31 C.F.R. §§ 1010.410 (e) (funds transfer recordkeeping for BSA financial institution and other banks) and 1010.410(f) (the Travel Rule).

**3.12 Is ownership of legal entities in the form of bearer shares permitted?**

Ownership in the form of bearer shares is not permitted for legal entities organized under the laws of the states of the U.S. There is no prohibition on providing financial services to entities whose shares are held or authorized to be held in bearer form, but as an AML practice many financial institutions prohibit or restrict relationships with legal entities whose shares are held in bearer form.

**3.13 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?**

There are three requirements with general applicability. As noted, all trades or businesses in the United States, unless designated as financial institutions under the BSA, are subject to cash reporting (Form 8300 reporting). *See* question 3.3. In addition, all persons (individuals and legal persons) are subject to cross-border (CMIR) reporting. *See* question 3.5. Also, under the BSA, all U.S. persons (individuals and legal persons) must report annually all foreign financial accounts valued at $10,000 or more in the aggregate at any point in the previous calendar year if they have an ownership interest in, or (with some exceptions) signatory authority over, the account. This is referred to as the FBAR requirement (Foreign Bank and Financial Accounts Report). 31 C.F.R. § 1010.350.

**3.14 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?**

Not routinely. Under the BSA, however, if there is a demonstrated law enforcement need, FinCEN can impose "geographic targeting" – temporary regulatory requirements for financial institutions or other trades or businesses to file reports or keep records with certain characteristics for a set period of time. 31 C.F.R. § 1010.370. For instance, currently, there is a Geographic Targeting Order in place in certain major metropolitan areas requiring reporting by title insurance companies on cash sales (non-financed sales) of residential real estate purchased by legal entities over a given threshold amount. This GTO is currently in effect and has been re-issued several times.

## 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. It is not clear at this time whether the proposal will be finalized. 80 Fed. Reg. 52680 (Sept. 1, 2015).

On April 4, 2016, FinCEN issued a Notice of Proposed Rulemaking in the Federal Reserve 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. 81 Fed. Reg. 19086. This proposal also has not been finalized.

FinCEN intends to finalize a proposed regulation that would impose certain BSA requirements on banks without a federal functional regulator, *i.e.*, banks and credit unions that are not federally insured, uninsured private banks, and a specialized class of financial institution licensed by Puerto Rico. This action was proposed on August 25, 2016. 81 Fed. Reg. 58425.

The same pending legislation referenced in question 3.10, above, also would make a number of improvements to the BSA.

**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 report on the 2016 FATF mutual evaluation of the United States and the FATF's March 2020 *3rd Enhanced Followup Report and Technical Compliance Re Rating*, 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, pending legislation would address FATF's criticism about the lack of a corporate registry with reliable beneficial ownership information. 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.

**4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?**

The United States was last evaluated by the Financial Action Task Force in 2016. The FATF report is available at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

**4.4 Please provide information for how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?**

The state and federal statutes cited are available from a number of internet sources. The federal regulations ("C.F.R.") are available at www.ecfr.gov. FinCEN, the federal functional regulators, and SROs all provide access to guidance, advisories, and public enforcement actions through their websites. The FinCEN website is particularly useful with links to statutes, regulations, and Federal Register notices, which provide helpful explanations of proposed and final regulations. *See, e.g.*, FinCEN, www.FINCEN.gov. As noted in question 2.5, the FFIEC manual sets forth extensive guidance for banks.

**Joel M. Cohen**, 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. Mr. Cohen is highly rated in *Chambers* and in *The Best Lawyers in America©*, a "Litigation Star" national Top 100 Trial Lawyer by *Benchmark Litigation*, an "MVP" by *Law360*, one of the world's leading practitioners in White Collar Crime in Euromoney's *Expert Guides – White Collar Crime*, a "Super Lawyer" in Criminal Litigation, in *The Legal 500*, and his work has been featured in *The American Lawyer* and the *National Law Journal*.

**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

**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 & 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

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.

**www.gibsondunn.com**

GIBSON DUNN

# ICLG.com

## Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
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
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms
Workplace Pensions

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group