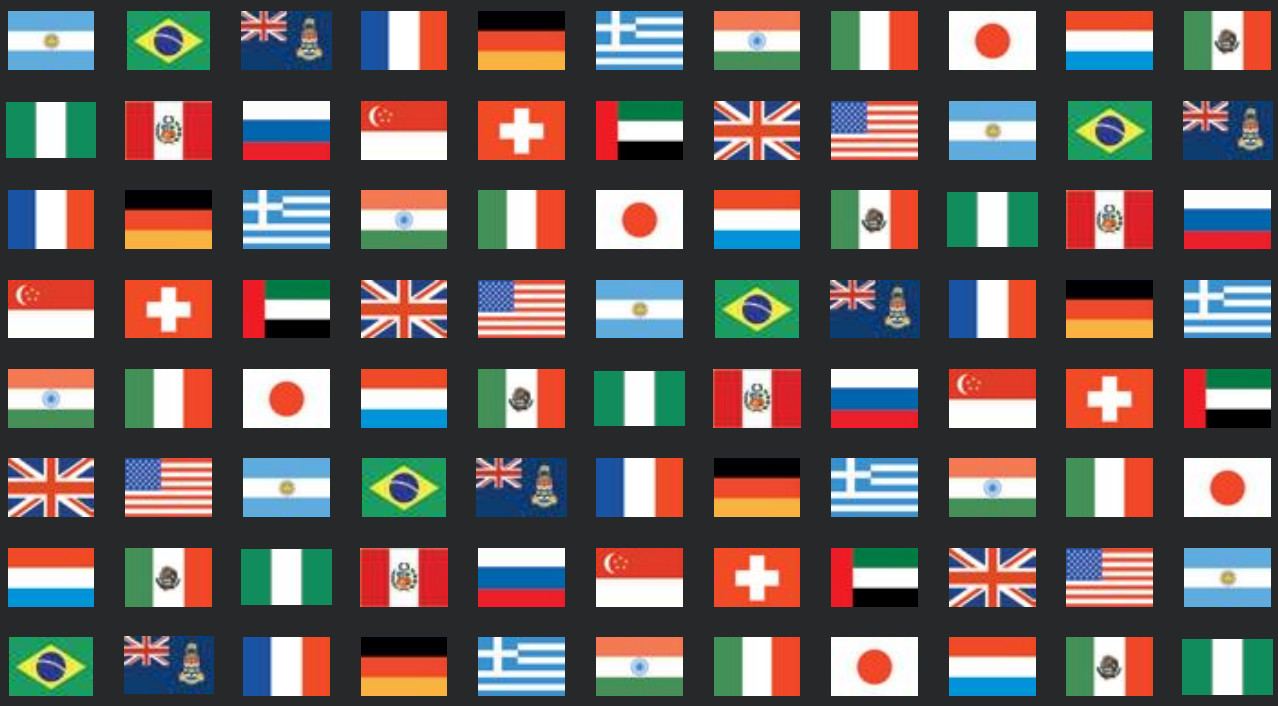
Anti-Money Laundering

Contributing editors
Lamia R Matta and Ann Sultan



2017

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Anti-Money Laundering 2017

Contributing editors

Lamia R Matta and Ann Sultan

Miller & Chevalier Chartered

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Sixth edition
ISSN 2050-747X

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Global overview

Lamia R Matta and Ann Sultan
Miller & Chevalier Chartered

Getting the Deal Through – Anti-Money Laundering aims to educate businesses about the numerous regimes for global and national anti-money laundering and combating the finance of terror (AML/CFT) operating around the globe.

We hope this publication will become part of the compliance arsenal that financial institutions (FIs) and multinational companies (MNCs) use to manage the risks inherent in doing business across international jurisdictions. However, it is only part of the arsenal, because AML/CFT laws are but one of the many compliance-related regimes that FIs and MNCs must understand as they go about their daily business.

Companies must ensure that there is a natural flow of information between personnel handling anti-corruption, trade controls and AML/CFT compliance. Those doing business across borders would do well to adopt a holistic approach to compliance programmes to keep themselves at the cutting edge of changing financial environments. In previous years, we have shared 10 fundamental elements of effective compliance programmes that FIs and MNCs can leverage to develop cross-competent programmes. Those were:

- corporate leadership that prioritises and popularises a company-wide culture of compliance;
- a corporate governance structure that includes compliance officials fluent in AML/CFT and related regulatory environments;
- ongoing compliance analyses that assess the risks inherent in a company's geographic footprint and business model and are broad enough to encompass AML/CFT and related risk areas;
- cross-disciplinary compliance policies that are developed, updated, promulgated and implemented via training on a consistent basis;
- methods to identify the multitude of entities and individuals with whom FIs and MNCs directly and indirectly transact, and target players that present significant risks in light of AML/CFT and related compliance guidelines;
- internal reporting mechanisms for employees and relevant third parties to report or otherwise surface AML/CFT and related issues, and effective internal protocols that trigger swift action in response to such reports;
- processes and structures to aggressively monitor and investigate conduct that implicates AML/CFT and related risk areas; for example, in-house financial intelligence units (FIUs) to monitor, investigate and analyse 'suspicious activity', or the establishment of dedicated groups of investigators and compliance personnel focused on AML/CFT and related regulatory burdens;
- processes for expeditiously assessing the magnitude of a particular compliance allegation and judiciously escalating concerns within the company hierarchy before gaming out the implications of disclosure required by AML laws;
- cross-disciplinary training and certification programmes in AML/CFT and related compliance areas; and
- a commitment to regularly test and audit cross-disciplinary compliance programmes, keeping in mind shifting AML/CFT landscapes.

In light of recently reported data breaches at major companies and the passing of the General Data Protection Regulation adopted by the European Union in April 2016, we add an 11th element to an effective compliance programme: effective data security protocols, systems and management. FIs and MNCs that are able to incorporate all of these elements into a cross-disciplinary compliance programme will be well positioned to manage the regulatory hurdles that governments across the globe are erecting to staunch the rise of money laundering activities and combat the financing of terrorism.

Previously, we noted that regulatory and enforcement agencies have renewed their focus on 'tone at the top', particularly in the United States. The reasoning behind the growing emphasis on individual responsibility for AML/CFT compliance at the top levels of company management, we explained, was to create personal liability in enforcement actions that involve corporate misconduct.

As the fight against terrorist financing continues around the world, we have seen increased efforts on the part of many governments to bolster anti-money laundering regulations and enforcement. For example, in March 2017 the UK government announced plans to set up a new anti-money laundering watchdog, the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) by the beginning of 2018. Taiwan, too, recently created a new government agency, the Anti-Money Laundering Office, to work on anti-money laundering efforts. Kenya enacted new anti-money laundering legislation and New Zealand is considering legislation that would be 'Phase 2' of the country's AML/CFT Act from 2013. In the US, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) instituted an enhanced customer due diligence requirement in May 2016 with which relevant financial institutions have until May 2018 to comply.

This year should also see the implementation of Directive (EU) 2015/849, also known as the Fourth Money Laundering Directive, which was adopted by the European Parliament on 20 May 2015, and which EU member state national legislatures have two years to implement. The Directive sought to implement the recommendations of the Financial Action Task Force (FATF). The FATF is an intergovernmental body tasked with examining money laundering techniques and trends, reviewing legislative and law enforcement actions relating to money laundering at the national and international levels, and issuing recommendations to combat money laundering and stem terrorist financing. As the European Commission noted in its press release on the Directive, the Directive is designed to contribute to the fight against money laundering and terrorist financing by:

- facilitating the work of Financial Intelligence Units from different member states to identify and follow suspicious transfers of money and facilitate the exchange of information;
- establishing a coherent policy towards non-EU countries that have deficient anti-money laundering and counter-terrorist financing regimes; and
- ensuring full traceability of funds transfers within, to and from the European Union.

Last year, members of the Egmont Group of Financial Intelligence Units (the Egmont Group) – an informal network of national FIUs that specialises in sharing and analysing global operational and strategic financial intelligence – produced an in-depth study of terrorist financing by Foreign Terrorist Fighters (FTSs) for the Islamic State of Iraq and the Levant (ISIL). Financial intelligence units that participated in the study were able to connect networks of FTF financial facilitators across jurisdictions, use shared information to identify new trends and develop new investigative leads for law enforcement.

On the heels of that report, the Egmont Group held an extraordinary meeting of its governing body to discuss recommendations for responding to the increased threat of terrorist financing. In February 2016, the Egmont Group announced that it had adopted a number of recommendations designed to work against the growing threat of FTFs, including to:

- provide indicators of terrorism financing to industry partners to help them identify suspicious financial activity;
- consider the reporting of couriers transporting cash or non-cash instruments across borders;
- expand the range of reporting entities subject to the Suspicious Transaction Reports reporting regime; and
- examine the utility of cross-border wire transfer information in the context of combating terrorist financing.

At its 2017 annual meeting, the Egmont group extended its global reach by welcoming three additional members to its ranks. Several countries also executed new bilateral information-sharing agreements.

Another significant development in the investigation and prosecution of money laundering and terrorist financing has been the publication and analysis of the Panama Papers. In early 2015, an anonymous source known only as 'John Doe' leaked the 11.5 million documents to a German newspaper. The documents revealed detailed information about more than 200,000 offshore companies associated with the Panamanian law firm and corporate service provider Mossack Fonseca. Given the large numbers of documents at issue, the newspaper enlisted the help of the International Consortium of Investigative Journalists, which distributed the documents for analysis to journalists and media organisations worldwide. The resulting reports sparked global outrage, as it has become clear that some of the accounts were used to hide assets from national tax authorities, to launder money or to move wealth seamlessly between jurisdictions. A number of countries have announced investigations of the nationals – both companies and individuals – whose assets were held in the accounts, while some world leaders have stepped down after the leaks showed they held or were associated with shell companies used to evade taxes or otherwise hide money. Organisations involved in terror finance are known to have used offshore accounts, similar to ones set up by Mossack Fonseca, to funnel funds to FTFs. The Panama Papers revelations will no doubt generate further recommendations relating to terrorist financing. In the past year, governments and institutions in Australia, Austria, France, Iceland, India, Mexico, the Netherlands, Norway, Panama, Spain, Sweden and the United States, among others, have begun taking a wide range of actions against individuals, organisations and accounts linked with the Panama Papers. For example, the two founders of Mossack Fonseca – Ramon Fonseca and Jurgen Mossack – were arrested on money laundering charges after the Panama office of Mossack Fonseca was raided in connection with Brazil's 'Operation Car Wash' bribery and corruption investigation; the Royal Bank of Canada closed 40 accounts linked to the Panama Papers; Cyprus referred four law firms connected with the Panama Papers to a disciplinary council; and governments around the world are investigating individuals associated with the Panama Papers. There have been significant political ramifications as well: in April 2016, the Prime Minister of Iceland, Sigmundur Davið Gunnlaugsson, resigned after it was revealed that he and his wife had set up a company in the British Virgin Islands. Prime Ministers in Britain and Pakistan faced questions about family accounts as well.

Finally, a look at some of the unexpected consequences of the increased scrutiny on the operations and compliance systems of financial institutions: the global banking sector has, unsurprisingly, reacted with anxiety to the high penalties of recent AML/CFT investigations and resolutions. As a result, many banks – especially in the United States – have engaged in what is referred to as 'de-risking', or terminating relationships with foreign correspondent banks and other clients whose operations might pose a risk to complying with AML/CFT laws. Many institutions, including the World Bank and the Global Center on Cooperative Security, have pointed out that the approach has resulted in the isolation of certain communities from the global financial system and, ultimately, an undermining of AML/CFT objectives. Some regulatory authorities have announced that de-risking is a misapplication of the risk-based approach they recommend, and have sought to persuade financial institutions to proceed with a lighter touch. In November 2016, the International Monetary Fund noted that Caribbean countries faced a significant threat to their economies from the loss of correspondent banking relationships. In response, the Caribbean Development Bank has approved funding to assist members of the Organisation of Eastern Caribbean States to strengthen their implementation of and compliance with international financial integrity standards and increase banks' technical capabilities for customer due diligence, among other goals. The risk-based approach in limiting relationships may also be contributing to banks' lack of enthusiasm for doing business in Iran, even as the Joint Comprehensive Plan of Action (commonly referred to as the Iran Deal) is implemented, because of insufficient anti-money laundering controls in the Iranian financial system.

United States

Lamia R Matta and Ann Sultan
Miller & Chevalier Chartered

Domestic legislation

1 Domestic law

Identify your jurisdiction's money laundering and anti-money laundering (AML) laws and regulations. Describe the main elements of these laws.

The United States has a comprehensive set of money laundering and anti-money laundering (AML) laws and regulations at the federal and state level.

The cornerstone of the federal AML framework is the Bank Secrecy Act (BSA), 31 USC section 5311 et seq. Enacted in 1970, it was the first federal law to require financial institutions to assist US government agencies in detecting and preventing money laundering. The BSA imposes certain reporting and record-keeping requirements on covered financial institutions and persons, and it imposes civil and criminal penalties for violations of the Act.

The Money Laundering Control Act of 1986 (MLCA), 18 USC sections 1956–1957, criminalises money laundering at the federal level. The MLCA prohibits the knowing and intentional transportation or transfer of proceeds of specified unlawful activities (SUAs) and prohibits transactions involving property derived from SUAs. It also amended the BSA by introducing civil and criminal forfeiture for BSA violations.

During the 1990s, a series of AML laws were enacted that strengthened sanctions for BSA reporting violations, required suspicious activity reports (SARs), criminalised the operation of unregistered money services businesses (MSBs) and obligated banking agencies to develop AML training for examiners. The most significant recent legislative development in the AML context, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (the Patriot Act), was passed into law in the immediate aftermath of the terrorist attacks of 11 September 2001. The Patriot Act was intended to enhance the BSA and MLCA in order to strengthen the government's ability to prevent, detect and prosecute international money laundering and the financing of terrorism.

The Patriot Act amended the BSA to require financial institutions to establish enhanced and formalised AML programmes and policies. It also authorised the US Treasury Department to issue rules requiring financial institutions to comply with confidential information requests from law enforcement; added reporting rules regarding the filing of SARs; set forth minimum standards for programmes that financial institutions employ to identify and verify the identity of customers; and expanded the list of crimes comprising SUAs for the purposes of the MLCA.

In addition to the federal AML laws, 38 of the 50 US states have AML laws. Some of these state regimes merely establish reporting requirements, while others either mirror federal law (eg, New York), or, in some cases, are more stringent than federal law (eg, Arizona).

Money laundering

2 Criminal enforcement

Which government entities enforce your jurisdiction's money laundering laws?

At the federal level, the US Department of Justice (DOJ) is responsible for the investigation and prosecution of money laundering crimes. Most prosecutions are conducted in the location where the offence occurred by one of the DOJ's 94 US Attorneys' Offices (USAOs), which are the primary federal law enforcement offices in their respective locations. For large, complicated or international cases, the DOJ's Money Laundering and Asset Recovery Section (MLAR) may assist local USAOs with the prosecution of the case.

The US Internal Revenue Service's criminal investigation section, which is part of the US Treasury Department, also has investigative jurisdiction over money laundering crimes. The Drug Enforcement Administration (DEA) oversees AML operations conducted in connection with its effort to combat drug trafficking and drug violence. The Department of Homeland Security's Immigration and Customs Enforcement agency is responsible for investigating bulk cash smuggling, drug smuggling, alien trafficking and other money laundering-related activities that are associated with the illicit movement of persons across US borders. The United States Postal Service also has criminal investigative authority over money laundering offences.

Each state in the US has its own law enforcement establishment responsible for investigating and prosecuting state crime, including the state crime of money laundering.

3 Defendants

Can both natural and legal persons be prosecuted for money laundering?

Yes, both natural and legal persons can be prosecuted. Criminal penalties for violations of the federal money laundering laws include fines as well as imprisonment. Fines are commonly imposed on corporations for violating the criminal money laundering statutes, while natural persons are routinely penalised with both fines and imprisonment.

4 The offence of money laundering

What constitutes money laundering?

Federal law criminalises four types of money laundering activities (18 USC sections 1956–1957):

- basic money laundering;
- international money laundering, involving the transfer of criminal proceeds into or outside of the United States;
- money laundering related to an undercover 'sting' case; and
- knowingly spending more than US$10,000 in criminal proceeds.

Basic money laundering

Section 1956(a)(1) prohibits conducting a financial transaction (eg, a deposit, withdrawal, transfer, currency exchange, loan, extension of credit and purchase or sale of securities or other monetary instruments) with funds that a person knows (or is aware to a high probability) are the proceeds of unlawful activity:

- with the intent to promote an SUA;
- with the intent to evade taxation;
- knowing that such transaction is designed to conceal information about the funds, including the location, source, ownership or control of said funds; or
- knowing the transaction is designed to avoid AML reporting requirements.

International money laundering

Section 1956(a)(2) prohibits the international movement of funds with the intent to promote an SUA. It further criminalises such movement of funds when a person knows that the funds represent proceeds of unlawful activity and where the purpose of moving the funds internationally is to conceal information about the funds, including the location, source, ownership or control of said funds, or avoid AML reporting requirements.

Sting operations

Section 1956(a)(3) deals with undercover ('sting') investigations. It prohibits a person from transacting with funds believed to be SUA proceeds (eg, because an undercover agent represents them as such) when that person intends to:

- promote an SUA;
- conceal information about the funds, including the location, source, ownership or control of said funds; or
- avoid reporting requirements.

Money spending statute

Section 1957, often called the 'money spending statute', prohibits otherwise innocent financial transactions tainted by the unlawful origin of the property exchanged in the transaction. It criminalises monetary transactions over US$10,000 when a person knows that the funds are derived from general criminal activity, and the property is, in fact, derived from an SUA. In effect, the US$10,000 threshold amount replaces the mens rea elements of the money laundering offences set forth in section 1956.

5 Qualifying assets and transactions

Is there any limitation on the types of assets or transactions that can form the basis of a money laundering offence?

For basic money laundering offences under section 1956(a)(1), the statute refers generically to 'proceeds', and thus there is no limitation on the types of assets or transactions that can form the basis of a money laundering offence and there is no monetary threshold to prosecution. However, the international money laundering provision, section 1956(a)(2), does not refer to 'proceeds' and instead refers to 'a monetary instrument or funds', which has been interpreted to mean that section 1956(a)(2) does not apply to transactions involving certain properties such as precious stones, metal, art or other high-value goods. As mentioned above, the money spending statute, section 1957, does have a threshold amount of US$10,000, but there is no limitation on the type of asset that may qualify.

6 Predicate offences

Generally, what constitute predicate offences?

The federal criminal money laundering statutes reference an extensive list of predicate offences. The underlying predicate offences are catalogued in 18 USC section 1956(c)(7) and include all of the Racketeer Influenced and Corrupt Organization Law predicate offences listed in 18 USC section 1961(1). There are nearly 250 predicate offences for money laundering, including federal, state and foreign crimes. The list of state and federal predicate offences are similar – murder, kidnapping, bribery, drug trafficking, arson, robbery and so on. Certain foreign crimes can be predicate offences if there is a sufficient nexus between the conduct and the United States.

The list of federal predicate offences is expansive but does not currently include tax evasion, despite the 2012 Financial Action Task Force (FATF) Recommendations guidance that suggested for the first time that serious tax crimes should be considered predicate offences. US senators Patrick Leahy (D-VT) and Charles Grassley (R-IA) introduced legislation in 2011 that would include tax evasion in the list of predicate offences for money laundering prosecutions, but neither reintroduced the bill in subsequent sessions of Congress. Leahy has publicly supported the reintroduction of the bill in November 2014, but has not acted on it since. In April 2013, the US Senate Caucus on International Narcotics Control, chaired by US Senators Dianne Feinstein (D-CA) and Grassley issued a report, 'The Buck Stops Here: Improving US Anti-Money Laundering Practices', in which they encouraged the enactment of legislation such as the Incorporation Transparency and Law Enforcement Assistance Act, which would require the disclosure of beneficial ownership information to combat the use of anonymously incorporated shell companies, and the Combating Money Laundering, Terrorist Financing and Counterfeiting Act of 2011, which would make all felonies, including tax evasion, predicate offences for money laundering. Nothing came of the Combating Money Laundering, Terrorist Financing and Counterfeiting Act of 2011. The 'Incorporation Transparency' bill was reintroduced in both the House and the Senate in 2013 and again in 2016, but it never made it out of committee.

7 Defences

Are there any codified or common law defences to charges of money laundering?

There are no codified or common law defences to money laundering charges. A typical defence at trial is that the defendant lacked the requisite mens rea – in other words, that the defendant did not know the proceeds were derived from SUAs.

8 Resolutions and sanctions

What is the range of outcomes in criminal money laundering cases?

In the United States, prosecutorial discretion is paramount. Setting aside political pressures, which may be powerful but are non-binding, there is no circumstance under which a prosecutor at either the state or federal level is required to bring money laundering charges against any person or institution. Likewise, nothing prohibits a prosecutor from offering a defendant a plea agreement rather than pursuing a conviction at trial.

The sanctions for AML violations include:

- any violation of the basic money laundering, international money laundering, or sting operation provisions (section 1956) carries a maximum sentence of 20 years' imprisonment;
- a violation of the money spending statute (section 1957) carries a maximum sentence of 10 years; and
- a defendant's actual sentence is determined by the presiding judge using the benchmarks provided by the United States Sentencing Commission's Sentencing Guidelines (USSG), which take into account the severity of the crime, the amount of the proceeds involved, the predicate offences involved, and a number of other relevant factors.

In addition, violations of the basic money laundering and international money laundering provisions, 18 USC section 1956(a)(1)–(2), are punishable by a fine not exceeding the greater of US$500,000 or twice the value of the property involved in the offence. Sting operation violations, 18 USC section 1956(a)(3), are punishable by fines of not more than the greater of US$250,000 (US$500,000 for an organisation) or twice the value of the property involved in the offence. Violations of the money spending statute, 18 USC section 1957, are punishable by a fine not exceeding the greater of US$250,000 or twice the value of the property involved in the offence.

9 Forfeiture

Describe any related asset freezing, forfeiture, disgorgement and victim compensation laws.

There are three types of forfeiture proceedings in the United States:

- criminal forfeiture, 18 USC section 982;
- civil forfeiture, 18 USC section 981; and
- administrative or 'non-judicial civil' forfeiture, 18 USC section 983(a)(1)–(2) and 19 USC section 1607.

Criminal forfeiture
Criminal forfeiture is intended as a further penalty on the guilty party and is limited to the property interests of the defendant. As such, criminal forfeiture proceedings may only occur after the defendant is adjudicated guilty.

Forfeiture is statutorily required in money laundering prosecutions – for example, the presiding court, in imposing a sentence on a defendant pursuant to 18 USC sections 1956 or 1957, must order the defendant to forfeit to the United States 'any property, real or personal, involved in the offense, or any property traceable to such property'. Under 21 USC section 853(e)(1), the government may seek a pre- or post-indictment restraining order or injunction to preserve the availability of the property prior to judgment.

The government must notify a defendant upon charging of its intent to seek forfeiture in order for a court to enter a judgment of forfeiture upon a finding of guilt. A court must grant a forfeiture order if the government proves by a preponderance of the evidence that forfeiture of the property is warranted. If, upon conviction, the government is unable to access the defendant's interest in forfeitable assets, courts will order the forfeiture of substitute assets. For example, the Patriot Act permits the seizure of funds subject to forfeiture located in a foreign bank account by authorising the seizure of the foreign bank's funds that are held in a correspondent US account. The funds in the US account are seen as a substitute for the foreign deposit.

Civil forfeiture
Civil forfeiture actions are instituted by the federal government against 'property, real or personal, involved in a transaction or attempted transaction' in violation of 18 USC sections 1956, 1957, or 1960, or 'any property traceable to such property'. The procedures established for civil forfeiture actions are complex but require that notice be provided to interested parties who are then given the opportunity to answer the government's complaint and defend the forfeiture on the merits.

Civil forfeiture actions may be brought concurrently with criminal forfeiture actions regarding the same property without triggering 'double jeopardy' protection. Prosecutors may switch from criminal to civil forfeiture if the requisite conditions for criminal forfeiture are not available.

Administrative/non-judicial civil forfeiture
Finally, administrative or 'non-judicial civil' forfeiture is available if no claims are filed contesting the forfeiture. The following four categories of property can be administratively forfeited:
- property that does not exceed US$500,000 in value;
- merchandise the importation of which is illegal;
- a conveyance used in moving or storing controlled substances; and
- currency or monetary instruments of any value.

Administrative forfeitures do not involve judicial authorities and comprise the vast majority of forfeiture actions.

10 Limitation periods

What are the limitation periods governing money laundering prosecutions?

The statute of limitations for money laundering prosecutions under 18 USC sections 1956 and 1957 is five years.

11 Extraterritorial reach

Do your jurisdiction's money laundering laws have extraterritorial reach?

There is extraterritorial jurisdiction for violations of 18 USC section 1956 if:
- the transaction or series of related transactions exceeds US$10,000; and
- the conduct is by a United States citizen or, if done by a foreign national, the conduct occurs in part in the United States.

In addition, there is extraterritorial jurisdiction for violations of 18 USC section 1957 under circumstances in which a US person (legal or natural) commits the offence outside of the United States.

Prior to the enactment of the Patriot Act, only a select group of foreign crimes were listed as predicates or SUAs for purposes of money laundering prosecutions under 18 USC sections 1956 and 1957. Section 315 of the Patriot Act expanded the list to include:
- any crime of violence;
- bribery of a public official;
- misappropriation of public funds;
- smuggling munitions or technology with military applications; and
- any 'offense with respect to which the United States would be obligated by multilateral treaty' to extradite or prosecute the offender.

As outlined in question 4, it is an offence to send money from any source into or out of the United States with the intent to promote one of the foreign predicate offences (18 USC section 1956(a)(2)(A)).

AML requirements for covered institutions and individuals

12 Enforcement and regulation

Which government entities enforce your jurisdiction's AML regime and regulate covered institutions and persons? Do the AML rules provide for ongoing and periodic assessments of covered institutions and persons?

There are various AML enforcement and regulatory authorities in the United States. The Financial Crimes Enforcement Network (FinCEN) is a bureau of the US Treasury that exercises regulatory functions under the BSA. Its primary functions are to assist federal and local law enforcement in the detection and analysis of financial crimes, and to coordinate between law enforcement and financial institutions. FinCEN also has civil enforcement authority under the BSA against domestic institutions. In addition, pursuant to section 311 of the Patriot Act, FinCEN is responsible for identifying foreign financial institutions, foreign jurisdictions, types of accounts or classes of transactions of 'primary money laundering concern', for which domestic financial institutions must undertake certain special measures.

Other government and non-government organisations are also tasked with the administration and enforcement of the BSA, including the US Securities and Exchange Commission (SEC), the New York Stock Exchange, the National Association of Securities Dealers, the Commodity Futures Trading Commission, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration and the Financial Industry Regulatory Authority.

Both the US Treasury and the DOJ share prosecutorial authority over civil BSA violations. The DOJ has prosecutorial authority over criminal BSA violations.

13 Covered institutions and persons

Which institutions and persons must carry out AML measures?

The BSA (and its accompanying regulations at 31 CFR Chapter X et seq) is the primary law that establishes which institutions and persons must carry out AML measures. The BSA's principal focus is on 'financial institutions', which, over the years and through various amendments, have been defined under 31 USC section 5312(a)(2) and (c)(1) broadly to cover traditional financial service providers – such as banks, credit unions and thrifts – but also securities broker-dealers and futures commission merchants (FCMs), mutual funds and other investment companies, certain investment advisers and commodity trading advisers, insurance companies, casinos, pawnbrokers, dealers of precious metals, MSBs and other businesses that have been deemed to be vulnerable to money laundering activities.

BSA requirements vary for different types of financial institutions, with the most extensive requirements being imposed on banks. FinCEN issues regulations pursuant to the BSA with respect to the various industries covered by the BSA. For example, to further the United States' commitments in the G8 Action Plan of Company Ownership and Control, FinCEN issued its Final Rule on Customer Due Diligence (CDD) on 5 May 2016, requiring financial institutions – including banks, brokers or dealers in securities, mutual funds, futures commission merchants, and brokers in commodities – to collect information relating to the beneficial ownership of companies holding accounts in their institutions.

Beginning in May 2018, financial institutions will have to identify and verify the identity of any individual who owns 25 per cent or more of a legal entity, and any individual who controls the legal entity. In addition, the Rule requires financial institutions to conduct ongoing monitoring of the beneficial owners to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Also in May 2016, the Department of Treasury proposed legislation to Congress that would require all companies formed in the US to report information about their beneficial owners to FinCEN, essentially creating a registry of beneficial ownership information for companies. Congress has, so far, not acted on the proposed legislation.

The Department of Treasury and the Internal Revenue Service (IRS) issued final regulations at the end of 2016 that require foreign-owned LLCs that have only one member and that do not elect to be treated as corporations for tax purposes – which up to now did not have to file a separate tax return or obtain an Employer Identification Number – to obtain a tax identification number from the IRS, thereby requiring these entities to report ownership and transaction information to the IRS.

Finally, in February 2017, FinCEN renewed for another six months its geographic targeting orders, issued in March 2016, requiring US title insurance companies to identify the persons behind legal entities that are used to make cash purchases of high-end residential real estate transactions in certain parts of the United States. Prior to FinCEN's March 2016 action, US law did not impose reporting requirements on the real estate industry relating to the source of purchase funds or the beneficial owners of the real estate.

14 Compliance

Do the AML laws in your jurisdiction require covered institutions and persons to implement AML compliance programmes? What are the required elements of such programmes?

The Patriot Act amended the BSA to require that certain financial institutions establish AML compliance programmes. Such programmes must include, per 31 USC section 5318(h):

- internal policies, procedures and controls;
- the designation of a compliance officer;
- an ongoing employee training programme; and
- an independent audit function to test programmes.

In addition, and discussed in more detail below, US law imposes other AML obligations on covered institutions and persons such as:

- customer identification programmes (CIPs);
- monitoring and detecting suspicious activity;
- filing currency transaction reports (CTRs) and SARs;
- enhanced due diligence (EDD) on foreign correspondent accounts;
- a blanket prohibition on hosting correspondent accounts for foreign shell banks;
- mandatory information sharing in response to requests by federal law enforcement; and
- compliance with 'special measures' imposed by the US Treasury to manage particular AML concerns.

15 Breach of AML requirements

What constitutes breach of AML duties imposed by the law?

Financial institutions and persons subject to AML laws face penalties for failing to abide by BSA requirements. For example, the BSA prohibits the 'structuring' of a transaction with the purpose of evading an AML reporting or record-keeping requirement under 31 USC section 5324. To be found guilty of structuring, a defendant must:

- know that the financial institution has a reporting or record-keeping requirement;
- commit acts to evade that requirement; and
- intend to evade that requirement.

A classic example of a structuring offence occurs when a person tries to avoid financial reporting requirements triggered by cash transactions over US$10,000 by breaking up such a transaction into a series of smaller transactions at various financial institutions over the course of a few days (an activity known as 'smurfing').

In addition, the BSA imposes civil and criminal penalties for failing to file a required report, for filing a required report with a material omission or misstatement, and for failing to maintain records as required by the BSA, 31 USC sections 5321–22. Mere negligence is enough to trigger civil liability in these contexts, while criminal sanctions are reserved for wilful failures to abide by reporting requirements or records maintenance requirements.

Financial institutions that are required to file a report if they identify a suspicious transaction are prohibited from tipping off the subject of a suspicious transaction investigation. Institutions and persons who file SARs are protected from civil liability for filing such reports, but may not notify any person involved in the transaction that the transaction has been reported.

16 Customer and business partner due diligence

Describe due diligence requirements in your jurisdiction's AML regime.

The United States has adopted a risk-based approach in implementing its AML requirements generally. A financial institution's CDD processes should be commensurate with its AML risk profile and should be aimed at high-risk customers. Certain financial institutions are required to have a written CIP that must ensure that the financial institution takes reasonable steps to:

- establish the identity of the nominal and beneficial owners (eg, the individual or individuals who have a level of control over, or entitlement to, the funds or assets in an account) of a private banking account;
- determine if the account owner is a senior foreign political figure or someone affiliated with that figure (also known as a 'politically exposed person' or PEP);
- assess the sources of funds deposited into the account; and
- determine the purpose and expected use of the account (collectively termed 'know-your-customer' or KYC steps).

The CIP must also ensure that the financial institution monitors account activity to verify that such activity is consistent with the information known about the owner.

Accounts that have been identified by a financial institution's CDD programme as posing a heightened risk should be subjected to EDD procedures that are reasonably designed to enable compliance with AML requirements. For example, financial institutions that establish, maintain, administer or manage a private banking account or a correspondent account in the United States for a non-US person must establish EDD programmes 'that are reasonably designed to detect and report instances of money laundering through those accounts'.

As noted in the answer to question 13, FinCEN has issued a new rule that requires additional steps to identify beneficial owners.

17 High-risk categories of customers, business partners and transactions

Do your jurisdiction's AML rules require that covered institutions and persons conduct risk-based analyses? Which high-risk categories are specified?

US regulations deem high-risk customers to include:

- PEPs;
- foreign financial institutions;
- non-bank financial institutions;
- non-resident aliens and other non-US persons;
- foreign corporations with transaction accounts, particularly offshore corporations located in high-risk jurisdictions;
- deposit brokers;
- cash-intensive businesses;
- non-governmental organisations and charities; and
- professional service providers.

The EDD procedures for PEPs are generally the same as for other non-US holders of private banking accounts, but financial institutions have an additional obligation to develop procedures to reasonably identify and report transactions that might involve the proceeds of foreign corruption.

Section 313(a)(ii) of the Patriot Act and its corresponding regulations require financial institutions to take reasonable steps to ensure that correspondent accounts provided to foreign banks are not being used to provide banking services indirectly to foreign shell banks, defined as a foreign bank without a physical presence in any country. Financial institutions are required to obtain a certification from their foreign bank customers and to verify through re-certification every three years that the customer is neither a foreign shell bank nor a provider of financial services to foreign shell banks through US correspondent accounts. Each year, FinCEN issues an advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies. In September 2016, FinCEN provided guidance to FIs related to their EDD obligations for foreign correspondent accounts based on FATF's identification of jurisdictions that have strategic AML/CFT deficiencies and have not made sufficient progress in addressing the deficiencies. FinCEN advised US FIs that they should apply EDD procedures if they maintain correspondent accounts for foreign banks operating under a banking licence issued by the Democratic People's Republic of Korea and the Islamic Republic of Iran.

The United States also views cash transactions as posing serious money laundering risks. As a result, US authorities have implemented a declaration system called Reports of International Transportation of Currency or Monetary Instruments (CMIR). CMIR requirements apply to:

- persons who physically transport, mail, ship or cause to be physically transported, mailed or shipped, currency or other monetary instruments whose aggregate value exceeds US$10,000 on any one occasion to or from the United States; or
- persons in the United States who receive currency or other monetary instruments in excess of US$10,000 from a place outside the United States. Such persons are required to make truthful written declarations of such activities to the US Customs and Border Patrol (CBP). In addition, persons subject to US jurisdiction that receive currency exceeding US$10,000 in a trade or business must file reports with the IRS and FinCEN.

Trade-based money laundering (TBML) has also become a major concern among US AML authorities. Criminal organisations, particularly drug cartels, use the international trade system to transfer value across international borders and disguise the illicit origins of criminal proceeds. FinCEN has issued guidance to FIs to enable them to identify 'red flags' and report suspicious activities on their SAR forms as 'TBML' or 'BMPE' (black market peso exchange), but non-FIs are also at risk of becoming unwitting facilitators of TBML schemes.

18 Record-keeping and reporting requirements

Describe the record-keeping and reporting requirements for covered institutions and persons.

Financial institutions are required to file a number of different transaction reports to US AML authorities that rely on such reporting to identify and track illicit behaviour. These include:

- CTRs (31 CFR section 1010.311): a CTR must be filed each time a customer of a financial institution deposits, withdraws, exchanges, pays or transfers more than US$10,000 in currency.
- SARs: pursuant to 31 USC section 5318(g) and its corresponding regulations (eg, 31 CFR sections 1010.320, 1020.320, 1023.320 and 1024.320), financial institutions are required to report suspicious activity relating to both money laundering and terrorist financing. Covered institutions include banks, securities broker dealers, MSBs (except cheque cashers), FCMs, introducing brokers in commodities, insurance companies, mutual funds and casinos. The reporting threshold for non-MSB covered institutions is set at US$5,000; MSBs must file SARs when they involve at least US$2,000 (US$5,000 for issuers of money orders or travellers' cheques reviewing clearance records). Covered institutions required to file SARs must file a report if they know, suspect or have reason to suspect that:
  - the transaction involves funds derived from illegal activities;
  - the transaction is intended or conducted in order to hide or disguise funds or assets derived from illegal activities;
  - the transaction is designed to evade any regulations promulgated under the BSA, including structuring to avoid reporting thresholds;
  - the transaction has no business or apparent lawful purpose or is not the sort of transaction in which the customer normally engages; or
  - the financial institution knows of no reasonable explanation for the transaction after examining the available facts.
- Securities broker-dealers, insurance companies and MSBs must report transactions over the US$5,000 threshold in which they suspect they are being used to facilitate criminal activity generally. Also, banks have an obligation to file reports with respect to criminal violations involving insider abuse in any amount, criminal violations of US$5,000 or more when a suspect has been identified, and criminal violations of US$25,000 or more regardless of the identity of the suspect. Banks are encouraged to file a copy of their SARs with the state and local law enforcement authorities.
- Foreign banks and financial accounts report (FBAR) (31 CFR section 1010.350): an FBAR must be filed by any person subject to US jurisdiction who has a financial interest or authority over a financial account in a foreign country with an aggregate value of over US$10,000. The report must be submitted annually to the IRS.

In addition, all businesses and persons must file the following, as applicable:

- a report of transportation of currency or monetary instruments (31 CFR section 1010.340): this applies to any person subject to US jurisdiction that transports currency or any other monetary instrument valued at more than US$10,000; and
- a report relating to currency exceeding US$10,000 received in a trade or business (31 CFR section 1010.330): this applies to any person subject to US jurisdiction that receives currency exceeding US$10,000 in a trade or business.

Covered financial institutions and persons also have AML record-keeping obligations. These include:

- foreign financial accounts (31 CFR section 1010.420): a person subject to US jurisdiction is required to retain account records for any foreign financial account in which he or she has a financial interest. Such persons must keep records detailing the account's identifying information for a period of five years;
- extension of credit or transfer of funds over US$10,000 (31 CFR section 1010.410(a)): a financial institution extending credit or transferring currency, funds, cheques, investment securities, credit or other monetary instruments over US$10,000 must maintain the corresponding records. Such institutions must retain records for a period of five years identifying details of the transaction;
- transactions involving transfers over US$3,000 (31 CFR section 1020.410(a), (e)): with certain exceptions, a financial institution that transfers over US$3,000 must maintain records on the details of the transaction. This record-keeping requirement does not apply to transactions where both transmitter and recipient are: a bank, a broker or dealer in securities, an FCM or introducing broker in commodities, a wholly owned domestic subsidiary of the above, the United States, a state or local government, or a federal, state or local government agency or instrumentality; and
- CIP (31 CFR sections 1020.220, 1023.220, 1026.220): as part of their CIP and KYC programmes, financial institutions must collect identifying information about their customers and keep records of such information for five years after the customer's account is closed.

19 Privacy laws

Describe any privacy laws that affect record-keeping requirements, due diligence efforts and information sharing.

The United States does not have a general law of financial privacy as broad in scope as the various European laws enacted pursuant to the European Data Protection Directive. Rather, in response to the Supreme Court's pronouncement in *United States v Miller*, 425 US 435 (1976) that the US Constitution does not provide for a right to financial privacy, the US Congress enacted the Right to Financial Privacy Act (RFPA), 12 USC section 3401-22, a limited statute that establishes a framework for maintaining the confidentiality of financial information. The RFPA's goal is to protect individual customers – defined as natural persons or partnerships of five or fewer individuals – of financial institutions from unwarranted intrusion into their records by the federal government. The

RFPA's principal provisions prohibit a financial institution from releasing financial records of customers to the federal government. Various exceptions apply, including:

- when the customer authorises access;
- when an appropriate administrative or judicial subpoena or summons is issued;
- when a qualified search warrant is issued; or
- when there is an appropriate written request from an authorised government authority.

In addition, notice is not required when SARs are sent by FinCEN to law enforcement authorities.

In addition to the RFPA, in 1999 Congress enacted the Gramm-Leach-Bliley Act (GLBA), which grants the Federal Trade Commission (FTC) authority to issue rules requiring financial institutions to establish standards for security and confidentiality of customer records.

The GLBA also prohibits financial institutions from disclosing non-public personal information to unaffiliated third parties without providing customers with the opportunity to decline to have such information disclosed. The GLBA requires that financial institutions disclose their privacy policies to customers at the beginning of the business relationship and annually thereafter.

The Patriot Act, at section 314(a), requires certain financial institutions to respond to specific information requests from federal agencies through FinCEN, conduct record searches, and reply to FinCEN with positive record matches of targeted individuals or entities. Section 314(b) allows financial institutions that have adopted sufficient AML compliance programmes to share information with one another (upon providing notice to the Treasury Department) to identify and report to governmental authorities activities that may involve money laundering or terrorism.

Finally, the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 established the Consumer Financial Protection Bureau (CFPB) and consolidated the regulation and enforcement of financial privacy laws under the control of the CFPB.

20 Resolutions and sanctions

What is the range of outcomes in AML controversies? What are the possible sanctions for breach of AML laws?

Penalties for violating the BSA vary greatly, depending on a number of factors, including the type of violation at issue, the degree of wilfulness and the existence of prior violations. Sanctions available to FinCEN to resolve civil enforcement matters include letters of warning or caution, court-ordered injunctions or the imposition of consent orders. Where criminal penalties may attach, only the DOJ may file criminal charges against institutions in breach of AML laws. US federal judges have substantial leeway in determining penalties and will follow guidelines set forth in the USSG, in addition to the civil and criminal penalty provisions of the BSA.

Criminal penalties may be assessed for breaching a variety of AML laws. For example, institutions or persons who fail to file a CMIR, file a report containing a material omission or misstatement, or file a false or fraudulent report, may receive an administrative fine of a maximum of US$500,000, but may also be subject to a maximum period of incarceration of 10 years. Criminal penalties ranging from a fine of US$250,000 to a maximum sentence of five years' incarceration are also available for persons engaged in a trade or business who wilfully fail to file a FinCEN/IRS Form 8300 report upon receiving currency in amounts over US$10,000. Also, the Bulk Cash Smuggling statute, 31 USC section 5332, provides for criminal penalties of a maximum of five years' imprisonment for violations of the law as well as criminal and civil forfeiture.

In addition, FinCEN may assess civil monetary penalties for failing to file a CTR (eg, in violation of 31 CFR section 1010.311), for failing to file a SAR (eg, in violation of 31 CFR section 1010.320) or for failing to have an adequate AML compliance programme in place (eg, in violation of 31 CFR section 1020.210). Civil monetary penalties for wilful violations of AML laws and regulations such as these range from US$25,000 per violation (or per day without a proper compliance programme), to the actual amount involved in the violation, not to exceed US$100,000 per violation. For financial institutions that engage in a pattern of negligent violations of AML laws, FinCEN may impose civil monetary penalties of up to US$50,000.

Federal banking agencies (FBAs) – the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation – also have statutory authority to impose informal and formal administrative sanctions against the financial institutions whose activities they oversee. The most severe sanction an FBA may impose is to terminate the activities of a financial institution that has been found guilty of certain money laundering offences.

MSBs that fail to register with FinCEN, or file false or incomplete information in their registration statements, are subject to civil penalties of US$5,000 per day of non-compliance. Unlicensed MSBs are also subject to criminal fines and imprisonment of up to five years if persons carrying on such business knowingly fail to obtain a licence under 18 USC section 1960.

Covered institutions and persons in the securities sector who violate AML laws may be subject to civil penalties under the federal securities laws, enforced by the SEC, or may be subject to sanctions for violating self-regulatory organisation (SROs) internal rules. Enforcement remedies available to the SEC include cease-and-desist orders, court-ordered injunctions, censures or suspensions/bars from the securities industry and the assessment of civil monetary penalties. SROs may undertake their own enforcement actions as well.

21 Limitation periods

What are the limitation periods governing AML matters?

The statute of limitations for violations of AML laws subject to criminal penalties is typically five years.

22 Extraterritoriality

Do your jurisdiction's AML laws have extraterritorial reach?

Through its amendments to the BSA, the Patriot Act creates pressures on foreign institutions that ultimately arm the US authorities with international reach and influence. For example, the Patriot Act authorises the secretary of the treasury and the attorney general to subpoena records from a foreign bank that maintains a correspondent account with a US bank. Though the subpoenaed records must relate to the correspondent account, they may be located anywhere in the world. Should the foreign bank fail to comply with the subpoena, the US-based bank that maintains its correspondent account must terminate the account. As with any US-based subpoena recipient, foreign banks may initiate proceedings in a United States court to contest a subpoena.

It is not always possible for the US government to impose sanctions on foreign persons or institutions suspected of money laundering or financing international terrorism. Yet the Patriot Act has empowered the government to target such foreign persons and institutions by pressuring the financial intermediaries that provide them access to US markets.

The Patriot Act also requires US financial institutions to maintain CDD programmes that assess the risks associated with foreign bank correspondent accounts. The definition of a correspondent account under the Patriot Act is sufficiently broad to encompass most formal banking relationships between US and foreign banks. As a result, foreign banks wishing to avoid overly intrusive due diligence examinations from US financial institutions are incentivised to establish their own internal AML policies. In effect, the more stringent a foreign bank's AML detection programmes are, and the more robust a foreign bank's KYC efforts, the less likely US financial institutions are to adopt intrusive due diligence procedures in their dealings with the foreign bank.

Furthermore, the Patriot Act has created unprecedented seizure powers over funds located offshore. It permits the US government to seize funds subject to forfeiture but located out of reach in a foreign bank account by authorising the seizure of that foreign bank's funds that are held in a correspondent US account. This substitution is permitted regardless of whether the seized funds are traceable to the money held offshore in the foreign bank account.

Update and trends

The April 2016 publication of the so-called Panama Papers – a treasure trove of leaked documents showing detailed information about more than 200,000 offshore companies associated with the Panamanian law firm and corporate service provider Mossack Fonseca – brought a great deal of focus on the offshore banking industry and the attendant risks of money laundering. In the wake of those disclosures, the Obama administration announced a number of initiatives meant to crack down on the use of anonymous accounts, offshore secrecy and illicit financial transaction.

In May 2016, the Financial Crimes Enforcement Network (FinCEN) issued its Customer Due Diligence (CDD) Final Rule, which requires financial institutions – including banks, brokers or dealers in securities, mutual funds, futures commission merchants and brokers in commodities – to collect and verify the personal information of the beneficial owners who control or profit from companies that open accounts with the institutions. Also in May, the Department of Treasury proposed legislation to Congress that would require all companies formed in the United States to report information about their beneficial owners to FinCEN, essentially creating a registry of beneficial ownership information for companies. Similar legislation has long languished in the House and Senate, but there has never been sufficient momentum to turn these proposals into laws. With a new administration in the White House, and a different set of legislative priorities, it seems unlikely that such a registry will be created soon. In the fall of 2016, FinCEN issued a proposed rule to eliminate the anti-money laundering programme exemption for banks lacking a federal regulator. The rule would affect private banks, non-federally insured credit unions and certain trust companies and would require any entity that is considered a bank under federal rules to establish an AML programme. The deadline for comments, however, was October 2016 and FinCEN has yet to announce a final rule. At the end of 2016, the Department of Treasury and the Internal Revenue Service issued final regulations that require foreign-owned LLCs that register in any state in the United States or the District of Columbia, that have only one member and that do not elect to be treated as corporations for tax purposes – which up to now did not have to file a separate tax return or obtain an Employer Identification Number – to obtain a tax identification number from the IRS, thereby requiring these entities to report ownership and transaction information to the IRS.

In a development driven not by US policymakers, but by the international community, the Financial Action Task Force on Money Laundering (FATF) – an intergovernmental body developing and promoting policies to combat money laundering and terrorist financing – conducted its long-awaited assessment of the United States' AML regime. The findings, published in December 2016, were largely positive. The FATF noted that domestic coordination on AML/CFT issues has matured since the previous evaluation in 2006 and found that the AML/CFT framework in the United States is 'well-developed and robust'. However, the FATF noted in particular a gap in AML/CFT coverage over certain non-financial businesses and professions. The FATF recommended that AML/CFT rules be broadened to cover all investment advisers and that they be extended to lawyers, accountants, real estate agents, and trust and company service providers on a risk-based vulnerability analysis.

On the enforcement front, the United States, in one of the largest actions brought under the DOJ's Kleptocracy Asset Recovery Initiative, announced in July 2016 that it would seek to recover more than $1 billion in assets purchased with funds allegedly misappropriated from 1MDB, a Malaysian sovereign wealth fund. According to the DOJ, Malaysian officials misappropriated more than $3.5 billion from the fund and laundered the assets using 'a series of complex transactions and fraudulent shell companies with bank accounts located in Singapore, Switzerland, Luxembourg and the United States'. According to the DOJ, at least $1 billion traceable to the conspiracy was laundered in bank accounts in the United States.

The DOJ also announced in January 2017 that Western Union, a global money services business, agreed to forfeit $586 million to resolve DOJ and FTC investigations targeting the company's anti-fraud and AML programmes. The DOJ resolution included a deferred prosecution agreement in which Western Union admitted to helping people commit wire fraud and maintaining an ineffective AML programme. FinCEN assessed a $184 million penalty, which was deemed satisfied by the $586 million forfeiture.

The Financial Industry Regulatory Authority (FINRA) – an independent, not-for-profit organisation authorised by Congress to exercise oversight over the broker-dealer industry – was also very active in 2016. In May 2016, FINRA announced that it had fined Raymond James & Associates and Raymond James Financial Services a record $17 million for widespread failures relating to the their AML programme. FINRA also fined the firm's AML compliance officer, Linda Busby, $25,000 and suspended her licence for three months. Similarly, in December, FINRA fined Credit Suisse $16.5 million for AML and other violations.

The last year of the Obama administration saw a lot of activity on the AML/CFT front, in large part because there was a great deal of public scrutiny over offshore banking regulations and anonymous accounts. The open question for the coming year is how the new Administration will approach AML/CFT issues. Statements during the confirmation hearing of the Secretary of Treasury, Steven Mnuchin, gave no indication of significant deviation from long-standing US doctrine on AML/CFT. It is less clear how the Department of Justice enforcement agenda will evolve under the new Attorney General, Jeff Sessions. Many speculate that Sessions will be unwilling to antagonise Wall Street, but his or her history as a prosecutor at both the state and federal levels suggests otherwise. With the new administration focusing its efforts on anti-terrorism and national security, AML/CFT is sure to stay in the headlines for the year to come.

Civil claims

23 Civil claims and private enforcement

Enumerate and describe the required elements of a civil claim or private right of action against money launderers and covered institutions and persons in breach of AML laws.

Despite various attempts by private citizens to bring federal claims against financial institutions for failing to detect money laundering activities, the courts have ruled in those cases that the BSA and the Patriot Act do not provide a private right of action.

International anti-money laundering efforts

24 Supranational

List your jurisdiction's memberships of supranational organisations that address money laundering.

The United States joined the FATF in 1990.

25 Anti-money laundering assessments

Give details of any assessments of your jurisdiction's money laundering regime conducted by virtue of your membership of supranational organisations.

The FATF conducted its most recent assessment of the US's AML regime in January and February 2016 and published its findings in December 2016 in the Fourth Mutual Evaluation of the United States on Anti-Money Laundering and Counter-Terrorist Financing Measures (the 2016 Report). The 2016 Report provides a detailed summary of the United States' criminal money laundering laws and AML regime, and assesses the US system's strengths and weaknesses in light of the 40 FATF Recommendations, revised in February 2012. The FATF found that '[t]he AML/CFT framework in the US is well developed and robust'. It noted that '[d]omestic coordination and cooperation on AML/CFT issues is sophisticated and has matured since the previous evaluation in 2006'. The FATF found, however, that there are two overarching gaps in the US AML/CFT landscape that require action. The first is the '[l]ack of timely access to adequate, accurate and current beneficial ownership (BO) information'. The second is the gap in AML/CFT coverage over certain institutions and businesses such as investment advisers, lawyers, accountants, real estate agents, and trust and company service providers (other than trust companies). The FATF recommended that the US implement BO requirements under the BSA, scheduled to come into effect in 2018, and focus in particular

on applying AML/CFT obligations on investment advisers and, on the basis of a vulnerability analysis, to lawyers, accountants, and trust and company service providers.

26 FIUs

Give details of your jurisdiction's Financial Intelligence Unit (FIU).

FinCEN serves as the United States' FIU, and it is a founding member of the Egmont Group. FinCEN is contactable at:

Financial Crimes Enforcement Network
PO Box 39
Vienna, VA 22183
United States
Tel: +1 703 905 3591
www.fincen.gov

27 Mutual legal assistance

In which circumstances will your jurisdiction provide mutual legal assistance with respect to money laundering investigations? What are your jurisdiction's policies and procedures with respect to requests from foreign countries for identifying, freezing and seizing assets?

The United States provides mutual legal assistance to foreign law enforcement through all stages of money laundering investigations. The US has entered into numerous mutual legal assistance treaties (MLATs) and executive agreements with other countries in order to provide an expedited process for foreign countries to request and receive investigative assistance. Some MLATs apply to specific government agencies, such as the SEC, whereas other MLATs apply to specific types of crimes, such as drug trafficking, bribery, or tax evasion. Even without an MLAT, however, the United States may still provide legal assistance to foreign countries. Mutual legal assistance generally involves locating persons in the United States, compelling testimony and the production of evidence, and furnishing public records and financial data.

The DOJ and the State Department process most requests for such judicial assistance. Foreign legal attachés representing federal agencies abroad, such as the FBI, the DEA and the CBP, also accept and process requests for investigate assistance.

US law permits federal courts to receive requests directly from foreign countries for investigative assistance. While US federal courts receive most requests for mutual legal assistance, US state courts also may provide similar assistance. The courts assist foreign AML investigations by compelling testimony and the production of evidence.

In addition to providing investigative assistance, the United States can transfer forfeited assets to a foreign country, subject to certain statutory requirements. Specifically:

- the transfer must be agreed to by the DOJ and the Treasury Department;
- the Secretary of State must approve the transfer;
- an international agreement between the United States and the foreign country must authorise the transfer; and
- the foreign country must be certified under the Foreign Assistance Act of 1961 (if required).

The United States has received forfeited assets from Antigua and Barbuda, the Bahamas, Canada, Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Singapore, Switzerland and the United Kingdom. The United States has shared foreign assets with Anguilla, Antigua and Barbuda, Argentina, Aruba, Australia, the Bahamas, Barbados, Belgium, Bermuda, British Virgin Islands, Brazil, Canada, Cayman Islands, China, Colombia, Costa Rica, the Dominican Republic, Ecuador, Egypt, Germany, Greece, Guatemala, Guernsey, Honduras, Hong Kong, Hungary, Indonesia, Ireland, Isle of Man, Israel, Japan, Jersey, Jordan, Liechtenstein, Luxembourg, Malta, Mexico, the Netherlands, the Netherlands Antilles, Nicaragua, Palau, Panama, Paraguay, Peru, Philippines, Portugal, Qatar, Romania, South Africa, St Vincent and the Grenadines, Switzerland, Thailand, Turkey, the United Kingdom, Uruguay, Venezuela and Vietnam.

Miller & Chevalier

Lamia R Matta **lmatta@milchev.com**
Ann Sultan **asultan@milchev.com**

900 16th Street NW
Washington, DC 20006
United States

Tel: +1 202 626 5800
Fax: +1 202 626 5801
www.millerchevalier.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Anti-Money Laundering
ISSN 2050-747X

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law