GETTING THE DEAL THROUGH

Anti-Money Laundering

in 19 jurisdictions worldwide

2013

Contributing editors: James G Tillen and Laura Billings

Published by
Getting the Deal Through
in association with:

Anagnostopoulos Criminal Law & Litigation

Anderson Mōri & Tomotsune

Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW)

Ashurst Australia

AZB & Partners

Conlin Bedard LLP

Financial Action Task Force

Gorrissen Federspiel

Ivanyan & Partners

Maestre & Co Advocats

Miller & Chevalier Chartered

Niederer Kraft & Frey Ltd

Rubio Villegas y Asociados, SC

Simmons & Simmons

Sjöcrona Van Stigt Advocaten

Sofunde, Osakwe, Ogundipe & Belgore

Studio Legale Pisano

The Law Firm of Salah Al-Hejailan

Wilson Harle

Zingales & Pagotto Advogados (ZISP Law)

GETTING THE DEAL THROUGH®

Anti-Money Laundering 2013

Contributing editors
James G Tillen and Laura Billings
Miller & Chevalier Chartered

Business development managers
Alan Lee
George Ingledew
Dan White

Marketing managers
Rachel Nurse
Zosia Demkowicz

Marketing assistants
Megan Friedman
Cady Atkinson
Robin Synnot
Joe Rush

Administrative assistants
Parween Bains
Sophie Hickey

Subscriptions manager
Rachel Nurse
subscriptions@gettingthedealthrough.com

Head of editorial production
Adam Myers
Production coordinator
Lydia Gerges

Senior production editor
Jonathan Cowie
Production editor
Martin Forrest

Chief subeditor
Jonathan Allen
Senior subeditor
Caroline Rawson

Editor-in-chief
Callum Campbell
Publisher
Richard Davey

Anti-Money Laundering 2013
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

© Law Business Research Ltd 2013
No photocopying: copyright licences do not apply.

First published 2012
Second edition 2013
ISSN 2050-747X

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. No legal advice is being given in the publication. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of May 2013, be advised that this is a developing area.

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

Law Business Research

CONTENTS

Avoiding the Domino Effect: Keeping Abreast of the Global AML/CFT Legal and Regulatory Landscape
James G Tillen, Laura Billings and Jonathan Kossak *Miller & Chevalier Chartered* **3**

Effectiveness at the Top of the FATF Agenda The Secretariat *Financial Action Task Force* **5**

Andorra Marc Maestre Maestre & Co Advocats **7**

Australia Philip Trinca and Lisa Simmons Ashurst Australia **12**

Brazil Leopoldo Pagotto *Zingales & Pagotto Advogados (ZISP Law)* **18**

Canada Benjamin P Bedard and Paul D Conlin *Conlin Bedard LLP* **24**

Denmark Anne Birgitte Gammeljord *Gorrissen Federspiel* **30**

Greece Ilias G Anagnostopoulos and Jerina (Gerasimoula) Zapanti
Anagnostopoulos Criminal Law & Litigation **34**

India Aditya Bhat and Richa Roy *AZB & Partners* **40**

Italy Roberto Pisano and Chiara Cimino *Studio Legale Pisano* **50**

Japan Yoshihiro Kai *Anderson Mōri & Tomotsune* **59**

Mexico Juan Carlos Partida Poblador, Alejandro Montes Jacob and Marcela Trujillo Zepeda
Rubio Villegas y Asociados, SC **64**

Netherlands Enide Z Perez and Max J N Vermeij *Sjöcrona Van Stigt Advocaten* **70**

New Zealand Gary Hughes and Felicity Monteiro *Wilson Harle* **77**

Nigeria Babajide O Ogundipe and Chukwuma Ezediaro
Sofunde, Osakwe, Ogundipe & Belgore **85**

Philippines Chrysilla Carissa P Bautista
Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW) **89**

Russia Vasily Torkanovskiy *Ivanyan & Partners* **97**

Saudi Arabia Robert Thoms and Sultan Al-Hejailan *The Law Firm of Salah Al-Hejailan* **105**

Switzerland Adrian W Kammerer and Thomas A Frick Niederer Kraft & Frey Ltd **109**

United Kingdom Nick Benwell, Cherie Spinks, Emily Agnoli and David Bridge
Simmons & Simmons **116**

United States James G Tillen, Laura Billings and Jonathan Kossak
Miller & Chevalier Chartered **124**

Avoiding the Domino Effect:

Keeping Abreast of the Global AML/CFT Legal and Regulatory Landscape

James G Tillen, Laura Billings and Jonathan Kossak

Miller & Chevalier Chartered

In this, its second year of publication, ***Getting the Deal Through***'s *Anti-Money Laundering* reference book continues its mission of educating both financial institutions (FIs) and multi-national corporations (MNCs) regarding the global network of anti-money laundering and combating of the financing of terrorism (AML/CFT) regimes that have been established to disrupt the flow of illicit financing for criminal and terrorist individuals and organisations as well as rogue nations.

In last year's overview, we examined the history of the global AML/CFT legal and regulatory framework that has grown up alongside, and often struggled to keep pace with, the expansion of world-wide capital markets. We discussed the birth in 1974 of the Basel Committee, composed of 10 central bank governors, which develops broad supervisory standards and guidelines for financial authorities and recommends best practices. The Basel Committee's latest set of global standards remains its 2009 guidance, known as 'Basel III', which was meant to address the individual and systemic risks in the financial industry that were exposed during the financial crisis of 2008. We also underscored, as a primary source of AML/CFT guidance and reporting, the Financial Action Task Force (FATF), developed in 1989 by the leaders of the G7 Summit as an inter-governmental body tasked with the responsibility for examining money laundering techniques and trends, reviewing previous efforts, and setting out new measures to combat money laundering. FATF's renowned '40+9 Recommendations' were revised, simplified and consolidated into a new guidance publication, 'FATF Recommendations 2012', in February 2012 to further strengthen international standards for managing the threat posed by money laundering and financial terrorism activities. The consolidated FATF Recommendations include new focus areas, such as combating the financing of weapons of mass destruction; expanding the circle of politically exposed persons (PEPs) for any given country to include not only foreign, but also domestic officials, agents of international organisations, as well as their family and close associates; and expanding the list of predicate offences for money laundering to include serious tax crimes.

In addition to the Basel Committee and the FATF, we reviewed other inter-governmental bodies, such as the Egmont Group, which developed the notion of a centralised national agency responsible for coordinating the analysis and dissemination of financial information nationally and across borders, known as a financial intelligence unit (FIU); the United Nations Convention Against Transnational Organized Crime (Palermo Convention) of 2000; and the United Nations Convention Against Corruption of 2003, which adopted the notion of an FIU and urged member states, among other measures, to combat money laundering and work to improve the exchange of information internationally. The Palermo Convention entered into force on 29 September 2003, and currently has 147 signatories and 174 parties that have ratified, accepted, approved or acceded to the Convention. The Convention against Corruption entered into force on 14 December 2005, and currently has 140 signatories and 165 parties that have ratified, accepted, approved or acceded to that Convention. The European Commission is also engaged in updating and enhancing EU-level AML legislation and published in February 2013 its Fourth Money Laundering Directive draft legislation that adopts FATF's revised and consolidated 2012 recommendations.

Despite the general sense that these inter-governmental bodies often have little effect on the realities of the global financial world, FIs and MNCs ignore them at their peril. A perfect case study of the importance of reviewing AML/CFT reports and guidance can be seen in HSBC's December 2012 deferred prosecution agreement (DPA) with the United States Department of Justice (USDoJ), in which the large, UK-headquartered bank agreed to pay US$1.9 billion (including forfeiture of US$1.256 billion and a civil fine of US$650 million) to settle charges that it violated the US Bank Secrecy Act (BSA), International Emergency Economic Powers Act (IEEPA) and Trading with the Enemy Act (TWEA) between 2006 and 2010. HSBC's AML and trade sanction problems allegedly resulted from its failure to implement an adequate compliance programme capable of monitoring suspicious transactions and activities from its world-wide affiliates, particularly in Mexico. Most significantly, HSBC reportedly assigned Mexico its lowest AML risk rating, despite widely known evidence that doing business in Mexico carried serious risks. For example, recent FATF reports have indicated that more than 20 years since the criminalisation of money laundering in 1989, Mexican authorities have succeeded in obtaining only 25 convictions for the offence, despite the well-reported existence of the so-called Black Market Peso Exchange (BPME), a complex money laundering system that was developed as early as the late 1980s to enable the transfer of sales proceeds from the illicit drug trade in the United States to drug cartels outside the United States in countries such as Mexico and Columbia.

Due to HSBC's alleged failure to appreciate the risks of providing financial services in a region well-known for drug trade activities, the company neglected to monitor exchanges of over US$670 billion in wire transfers and over US$9.4 billion in purchases of US currency between its affiliates in Mexico and the United States from 2006 to 2010. According to US authorities, HSBC Mexico came to be considered the preferred FI for illegal drug cartels and money launderers during this period, in which approximately US$881 million in drug trafficking proceeds allegedly were laundered through HSBC's affiliates in Mexico and the United States. Even more troubling, the USDoJ alleged that HSBC's corporate headquarters was aware of the deficiencies in its Mexican affiliate's AML compliance programme and never informed its US affiliate of such weaknesses.

HSBC's alleged lax AML and trade sanction compliance programmes also resulted in serious violations of US trade sanctions laws. For over a decade prior to 2006, HSBC reportedly permitted sanctioned entities from Iran, Cuba, Sudan, Libya and Burma to omit their names from US dollar payment messages sent to HSBC's US affiliate and other FIs in the United States. According to US authorities, HSBC also inserted payment messages from sanctioned entities within Iran in such a way that the company's automatic filters were circumvented and precluded from blocking prohibited payments. Compliance officers at HSBC's US affiliate allegedly told their corporate headquarters that they would not be able to properly screen sanctioned entity payments if payment messages were opaque, but these warnings were not heeded.

HSBC was not the only company with headquarters outside the United States that was required to forfeit substantial sums of money to US enforcement agencies in 2012. In June, ING Bank NV, a financial institution with headquarters in Amsterdam, agreed to forfeit US$619 million for violations of the IEEPA and the TWEA, including illegally funnelling nearly US$2 billion through the US financial system on behalf of sanctioned Cuban and Iranian entities. Then in December 2012, Standard Chartered, a British banking institution, announced its own US$330 million settlement with the USDoJ for violating US economic sanctions against Iran by hiding the source (banned Iranian entities) of hundreds of billions of dollars worth of financial transactions. The bank's settlement with US federal authorities came only months after Standard Chartered settled claims based on similar activity with New York state regulators for US$340 million.

For FIs and MNCs doing business across the globe, the risk of an inadequate AML/CFT and trade sanction programme may be multiplied by the growing number of jurisdictions with potent enforcement regimes. For example, in 2012, South Korea's financial regulator, the Financial Supervisory Service, announced that it had launched investigations into activity by both HSBC's and Standard Chartered's South Korean affiliates, even though there was little to indicate that the South Korean branches of either of those companies were involved in any wrongdoing; the US enforcement actions were enough to provoke South Korean authorities to undertake their own investigations. Similarly, in August 2012, the United Arab Emirates's Dubai Financial Services Authority, which regulates firms operating in the UAE's financial free zone, made its own informal inquiries into Standard Chartered's branch activities in the region after learning of allegations by US authorities that the company had routed nearly half of its suspicious transactions through Standard Chartered's Dubai branch offices. And in March 2013, Argentine regulators announced charges against HSBC for money laundering and tax evasion in connection with operations unrelated to the company's settlement with the United States, but coloured by reports of HSBC's allegedly poor AML compliance programmes.

To avoid falling victim to an enforcement domino-effect where one jurisdiction's investigation causes a cascade of follow-on investigations by other jurisdictions, FIs and MNCs must keep up with the latest in AML/CFT compliance. This publication aims to be part of the compliance arsenal that FIs and MNCs should use to manage the risks inherent in doing business across international jurisdictions.

AML/CFT laws are just one of the many compliance-related regimes that FIs and MNCs must understand as they go about their daily business. Practically, this means that a siloed approach to AML/CFT compliance and related risk areas, such as anti-corruption and trade controls compliance, is no longer viable. For example, HSBC's AML and trade controls problems were the result of a lax attitude towards compliance overall; it was no coincidence that the company had serious compliance failures in both areas at the same time. Instead, companies doing business across borders would do well to adopt a holistic approach to compliance programmes. Effective compliance programmes share 10 fundamental elements that FIs and MNCs can use to develop cross-competent programmes:

- corporate leadership that prioritises and popularises a company-wide culture of compliance;
- a corporate governance structure inclusive of compliance officials fluent in AML/CFT and related regulatory environments;
- ongoing compliance analyses that assess the risk inherent in a company's geographical footprint and business model and are broad enough to encompass AML/CFT and related risk areas;
- cross-disciplinary compliance policies that are developed, 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 who 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 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.

FIs and MNCs that are able to incorporate these elements into a holistic cross-disciplinary compliance programme will be well positioned to manage the regulatory hurdles that countries across the globe are erecting to staunch the rise of money laundering activities and combat the financing of terrorism. This publication will continue to be updated annually and its coverage expanded to additional countries so that it may serve as a resource for FI and MNC compliance departments to use in order to educate themselves on the latest changes to the AML/CFT regulatory environment throughout the world.

United States

James G Tillen, Laura Billings and Jonathan Kossak

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 imposes civil and criminal penalties for violations of the Act.

The Money Laundering Control Act of 1986 (MLCA), 18 USC sections 1956–1957, criminalised 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 required 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 (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 through its investigative arm, the Federal Bureau of Investigation (FBI), 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 Asset Forfeiture and Money Laundering Section (AFMLS) may assist local USAOs or the DoJ's criminal division with the prosecution of the case.

The US Internal Revenue Service's criminal investigation section (IRS-CI), 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 (DHS) Immigration and Customs Enforcement (ICE) 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 (USPS) 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 a 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 a 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 (RICO) 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 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 such legislation has not been enacted into law.

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 of not more than 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 of not more than 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 'nonjudicial 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 to be 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/nonjudicial civil forfeiture

Finally, administrative or 'nonjudicial 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 which is illegal to import;
- 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 the response to 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?

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 has limited enforcement powers, but recently gained a new director, Jennifer Shasky Calvery, who began her career as a federal prosecutor investigating a multi-billion dollar money laundering scheme at Bank of New York involving suspected Russian Mafia money, and eventually became chief of the USDOJ's AFML Section, where she oversaw a programme that was responsible for the annual forfeiture of nearly US$1.5 billion in criminal assets. Given Director Shasky Calvery's enforcement background and expertise on shell companies and the dangers they pose for the financial system, the expectation is that FinCEN will be more aggressive in its enforcement and regulation of financial institutions (FIs), with a particular focus on expanding the requirements for FI due diligence investigations of accounts held by shell companies and other non-transparent entities.

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 (NYSE), the National Association of Securities Dealers (NASD), the Commodity Futures Trading Commission (CFTC), 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 (FINRA).

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, has 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 (CTAs), 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. Most recently, in March 2013, FinCEN issued guidance on the regulatory treatment of convertible 'virtual' currencies. Virtual currency is a medium of exchange that acts like real currency, but does not have legal tender status in any jurisdiction. It is considered convertible if it has an equivalent value in real currency or acts as a substitute for real currency. FinCEN's new guidance covers 'administrators', defined as persons engaged as a business in issuing a virtual currency and who have the authority to redeem such virtual currency and 'exchangers', persons who are engaged in the business of exchanging virtual currency for real currency, funds, or other virtual currency. FinCEN now treats administrators and exchangers of virtual currency as MSBs, thereby imposing on them MSB registration, reporting and record keeping requirements. The BSA's application to new industries will continue to broaden as new vulnerabilities are exposed.

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, 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 customer due diligence (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, which must ensure that the financial institution takes reasonable steps to:

- establish the identity of the nominal and beneficial owners (eg, 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 in order 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.'

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. In July 2012, FinCEN provided guidance to FIs related to their EDD obligations for foreign correspondent accounts based on FATF's June 2012 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 Bolivia, Cuba, Ecuador, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, Sao Tome and Principe, Sri Lanka, Syria, Tanzania, Thailand, Turkey, Vietnam, and Yemen.

The United States also views cash transactions as posing serious money laundering risk. 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 'BPME' (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 who rely on such reporting to identify and track illicit behaviour. These include:

- Currency Transaction Report (CTR) (31 CFR section 1010.311): a CTR is a filing triggered each time a financial institution deposits, withdraws, exchanges, pays, or transfers more than US$10,000 in currency;
- SAR: pursuant to 31 USC section 5318(g) and its corresponding regulations (eg, 31 CFR sections 1010.320, 1020.320, 1023.320, 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. Reporting thresholds 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;
  - the financial institution knows of no reasonable explanation for the transaction after examining the available facts; or
- Foreign 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, 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. In addition, 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.

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 transfers 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 of funds 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 section 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 recordkeeping 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 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 relatively recent enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), 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 willfulness, and the existence of previous 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 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 an 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 (OCC), the Board of Governors of the Federal Reserve System (Fed) and the Federal Deposit Insurance Corporation (FDIC) – 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.

Update and trends

The DoJ has had a string of recent successes in uncovering and disrupting the money laundering activities of drug-traffickers, criminal and terrorist organisations and trade-sanctioned entities through the investigation and prosecution of global financial institutions that acted as facilitators and conduits of such money laundering. These enforcement actions are high priorities for US national security interests, and both US and foreign financial institutions face intense scrutiny over their AML/CFT and trade sanction compliance programmes. In December 2012, the large, UK-headquartered bank HSBC, signed a deferred prosecution agreement with the DoJ, in which the company agreed to pay US$1.9 billion (including forfeiture of US$1.256 billion and a civil fine of US$650 million) to settle charges that it violated the US's Bank Secrecy Act (BSA), International Emergency Economic Powers Act (IEEPA) and Trading with the Enemy Act (TWEA) between 2006 and 2010. HSBC's AML and trade sanction problems allegedly resulted from its failure to implement an adequate compliance programme capable of monitoring suspicious transactions and activities from its worldwide affiliates, particularly in Mexico. Due to HSBC's alleged failure to appreciate the risks of providing financial services in a region well-known for drug trade activities, the company neglected to monitor exchanges of over US$670 billion in wire transfers and over US$9.4 billion in purchases of US currency between its affiliates in Mexico and the United States from 2006 to 2010.

HSBC's alleged lax AML and trade sanction compliance programmes also resulted in serious violations of US trade sanctions laws. For over a decade prior to 2006, HSBC reportedly permitted sanctioned entities from Iran, Cuba, Sudan, Libya and Burma to omit their names from US dollar payment messages sent to HSBC's US affiliate and other FIs in the United States.

In addition to the HSBC settlement, in June 2012, ING Bank NV, a financial institution with headquarters in Amsterdam, agreed to forfeit US$619 million for violations of the IEEPA and the TWEA, including illegally funnelling nearly US$2 billion through the US financial system on behalf of sanctioned Cuban and Iranian entities. Then in December 2012, Standard Chartered, a British banking institution announced its own US$330 million settlement with the DoJ for violating US economic sanctions against Iran by hiding the source (banned Iranian entities) of hundreds of billions of dollars worth of financial transactions. The bank's settlement with federal authorities in the United States came only months after Standard Chartered settled claims based on similar activity with New York state regulators for US$340 million.

Finally, following enforcement and regulatory actions taken in 2011 against the Lebanese Canadian Bank (LCB), a foreign financial institution, for acting as a conduit through which funds for the Hizballah Lebanese group (designated a terrorist organisation by the US) were funnelled through the US financial system, the US Attorney for the Southern District of New York and the US DEA announced in August 2012 the seizure of US$150 million in connection with a civil money laundering and forfeiture complaint filed against the LCB. The seized funds were taken from a US correspondent account held by a foreign financial institution, the Banque Libano Francaise SAL (BLF), which held US$150 million in an escrow account in Lebanon that were marked as purchase price funds related to the sale of LCB to the Societe Generale de Banque au Liban in 2011. The successful seizure of funds in this case serves as an example of the great lengths to which the US government will go to separate terrorist and criminal organisations from their funds.

In addition to disrupting the financial networks of organised crime, drug traffickers, terrorists, and rogue nations, the US government has also been active in investigating and prosecuting businesses whose inadequate AML programmes permitted scam artists to use their services to fleece unsuspecting consumers in the United States. For example, in November 2012, MoneyGram International Inc, an MSB, agreed to forfeit US$100 million pursuant to a deferred prosecution agreement in which the company admitted to criminally aiding and abetting wire fraud and failing to maintain an effective AML programme. MoneyGram allegedly failed to implement AML policies and procedures that would have caused it to file the required SARs when victims reported fraud to MoneyGram on transactions over US$2,000, or when the company discovered that its agents were involved in the fraud.

In December 2012, a federal district court ordered e-gold, LTD (EGL), a company whose business involved exchanging real currency for precious metals held in electronic form, to forfeit nearly US$11 million in connection with EGL's 2008 plea agreement in which it admitted to charges of money laundering and operating an unlicensed money transmitting business. As part of the plea agreement, and in coordination with the US Secret Service, EGL identified nearly 13,000 forfeited electronic customer accounts containing funds derived from a variety of criminal offences, including child pornography, credit card fraud, identity theft, investment fraud and the sale of stolen or non-existent goods on the internet. Only 22 of the nearly 13,000 account holders contested the forfeiture action. The lack of transparency involved in these electronic accounts and their vulnerability to abuse made them popular conduits for money laundering. It is likely that the prosecution of companies such as EGL influenced FinCEN's decision to issue guidance in March 2013 that imposes on virtual currency providers the same registration, reporting, and record keeping requirements as typical MSBs.

Finally, in July 2012, the United States attorney for the Southern District of New York announced a settlement agreement with two offshore online poker companies, PokerStars and Full Tilt Poker, in which the companies agreed to forfeit US$547 million to settle charges that the companies used fraudulent methods to circumvent the federal ban against unlawful internet gambling and deceive financial institutions into processing payments on the poker companies' behalf. Primarily, the two online poker companies disguised payments received from US gamblers as payments to hundreds of non-existent online merchants and in this way deceived US banks into processing billions of dollars in payment transactions.

These enforcement actions reveal the US's multifaceted approach to combating AML/CFT and trade sanction violations – the *HSBC* case alone required coordination among the DoJ's Criminal Division, the US Attorney's Office for the Eastern District of New York, the US Immigration and Customs Enforcement Agency, the New York and Queens County District Attorney's Office, the Treasury Department's Office of Foreign Assets Control, the Office of the Comptroller of the Currency; the FBI and the IRS's Criminal Investigation Division. They also reveal the reach of US enforcement actions as most of these cases involved settlements with companies whose headquarters are outside the United States. Despite the deep budget cuts many federal agencies are facing in the current political climate, forfeiture actions of the sort described herein have helped fill the coffers of the DoJ's Assets of Forfeiture Fund, and are likely to continue to permit aggressive enforcement actions in the coming years.

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 are, 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.

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.

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 2006 and published its findings in the Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism (the 2006 Report). This assessment was the US's first mutual evaluation since 1997. The 2006 Report provided a detailed summary of the United States' criminal money laundering laws and AML regime, and assessed the US system's strengths and weaknesses in light of the FATF's 40+9 Recommendations. The FATF concluded that the United States made significant improvements in its criminal laws and AML regime and determined that the US was 'compliant' or 'largely compliant' with the vast majority of the recommendations. Ultimately, the 2006 Report found that, although the United States has developed an effective AML regime, there is room for improvement given that the framework lacks a legal obligation to undertake ongoing due diligence.

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 can be contacted at:
Financial Crimes Enforcement Network
PO Box 39
Vienna, VA 22183
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.

MILLER CHEVALIER

James G Tillen **jtillen@milchev.com**
Laura Billings **lbillings@milchev.com**
Jonathan Kossak **jkossak@milchev.com**

655 Fifteenth Street, NW
Suite 900
Washington, DC 20005-5701
United States

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

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 attaches 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, the Bahamas, Canada, the Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Singapore, Switzerland, and the United Kingdom. The United States has shared foreign assets with Aruba, Australia, the Bahamas, Brazil, the Cayman Islands, China, Dominican Republic, Egypt, Guernsey, Honduras, Isle of Man, Japan, Jersey, Mexico, the Netherlands, Nicaragua, Palau, Panama, Portugal, Qatar, St. Vincent and the Grenadines, Switzerland, the United Kingdom and Vietnam.

GETTING THE DEAL THROUGH®

Annual volumes published on:

Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Dispute Resolution
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Insurance & Reinsurance
Intellectual Property & Antitrust
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Shipbuilding
Shipping
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Vertical Agreements

For more information or to purchase books, please visit:
www.gettingthedealthrough.com

The Official Research Partner of the International Bar Association

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Strategic research partners of the ABA International section

ANTI-MONEY LAUNDERING 2013 ISSN 2050-747X