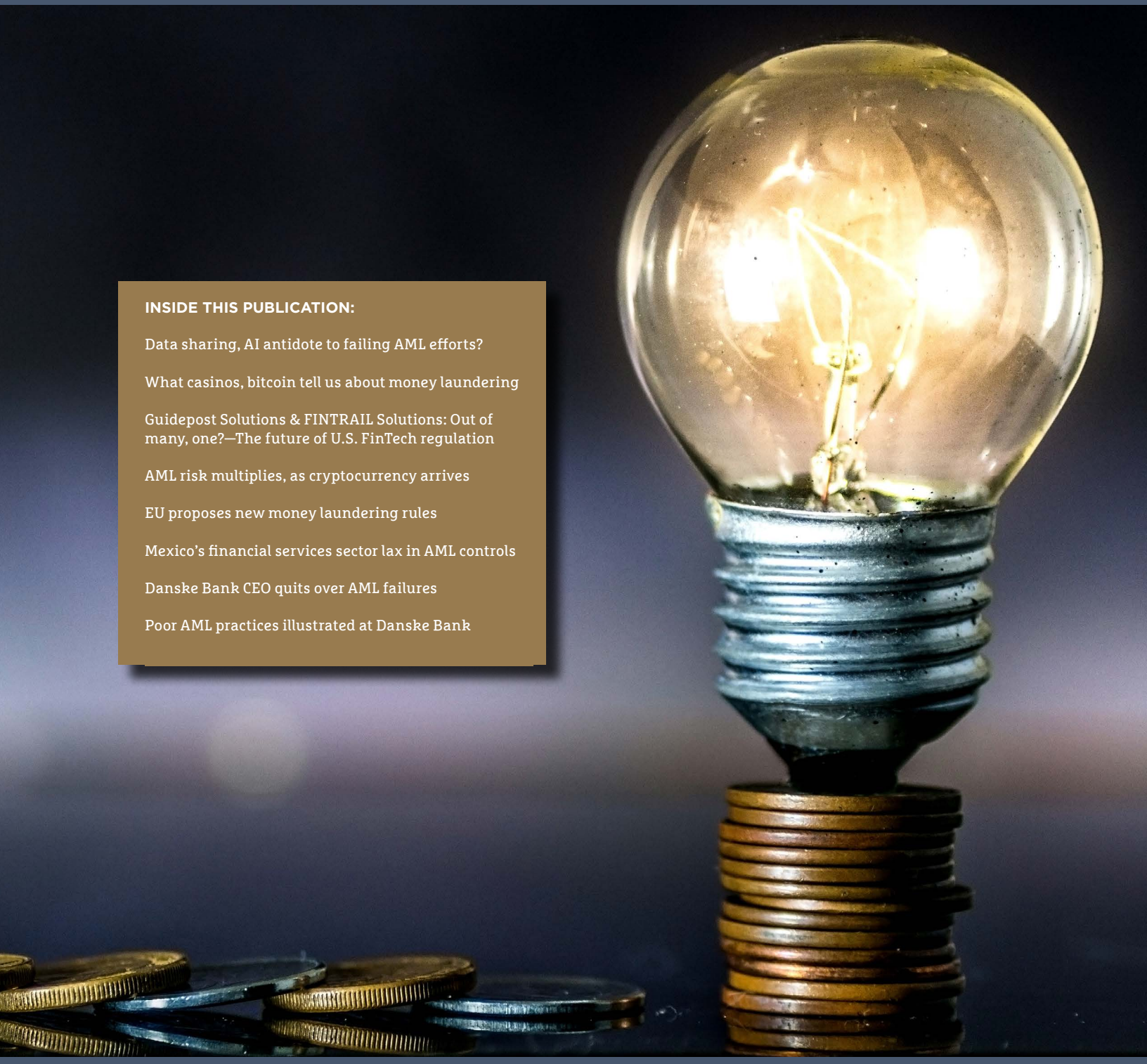
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Innovative ways to reduce Money laundering risk

Guidepost

FINTRAIL SOLUTIONS

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

Guidepost

In a world where change is certain, experience is the best protection. Guidepost Solutions offers global investigations, compliance and monitoring, and security and technology consulting solutions for clients in a wide range of industries. Our expert team provides leadership and strategic guidance to address critical client needs across the globe. Experience guides us. Solutions define us. For more information, please visit www.guidepostsolutions.com.

FINTRAIL SOLUTIONS

Guidepost Solutions LLC, a global leader in compliance, investigations, and security consulting, in conjunction with financial technology compliance consulting firm FINTRAIL LTD., launched FINTRAIL Solutions LLC, a financial crime consultancy company to offer North American FinTech and RegTech firms with specialized services to manage their risks and navigate the uncertainty of future regulations for themselves and their clients. For more information, please visit www.fintrailsolutions.com.

Inside this e-Book

Data sharing, AI antidote to failing AML efforts?

Big data may revolutionize anti-money laundering efforts, but privacy concerns and preserving a human element to compliance programs may get in the way. **Joe Mont** explores.

Despite the United States' prominence in the world of finance, its efforts to attack the root causes of money laundering are sorely lacking.

Suspicious activity reports, for example, are widely considered to be little more than very expensive busy work that, in a vacuum, rarely uncovers criminal activity.

In an age of political impasse, the need to update the Bank Secrecy Act and Anti-Money Laundering regulatory regimes has become a bipartisan cause. Among the ideas: resolving the privacy roadblocks to data sharing and using modern technology, including artificial intelligence and machine earning, to do the detective/grunt work.

To that end, Rep. Ed Royce (R-Calif.) introduced the Anti-Money Laundering Modernization Act of 2017 in September 2017.

"Our nation's anti-money laundering and countering terrorism financing regime has been a 40-year work in progress, and there is increasing recognition that it needs to be modernized," Royce said of the bill's introduction. "Our regulatory infrastructure must keep pace with the times. Criminal syndicates, rogue nations and terrorist networks are not sitting idly by, and neither can we."

The bill would also expand the ability of financial institutions to share suspicious activity reports within their organization to improve enterprise-wide risk management and require Treasury to improve qualitative feedback for financial institutions and Federal financial regulators on their AML/CTF efforts.

Importantly, the legislation would also require Treasury to explore the potential for artificial intelligence, machine learning, and other technologies to help detect and prevent money laundering and terrorist financing.

The prospect of applying AI and other technological advances to AML programs was also a recurring theme at a Jan. 9 hearing of the Senate Banking Committee.

At the hearing, Greg Baer, president of the Clearing House Association, laid out the many problems currently facing the nations AML regime.

"Our AML/CFT system is broken," he said. "A core problem is that today's regime is geared toward compliance expectations that bear little relationship to the actual goal of preventing or detecting financial crime … Fundamental change is required to make this system an effective law enforcement and national security tool, and reduce its collateral damage.

The regulatory regime, he said, "is a system in which banks have been deputized to act as quasi law-enforcement agencies and where the largest firms collectively spend billions of dollars each year, amounting to an annual budget somewhere between that of the ATF and the FBI."

Large banks, Baer said, have been pushed away from risk-based approaches, because their performance is not graded by law enforcement or national security officials, but rather by bank examiners.

"Those examiners focus on what they know and control: policies, procedures, and quantifiable metrics—for example, the number of computer alerts generated, the number of SARs filed, and the number of compliance employees hired," he added. "This means that a firm can have a program that is technically compliant, but is not effective at identifying suspicious activity, or is producing adverse collateral consequences."

As a result, he said, banks are filing SARs that are in less than 10 percent of cases followed up on in any way. For certain categories of SARs, the yield is close to 0 percent.

To put some numbers to the issue, Baer said that one AML director recently testified that his firm employs 800 individuals worldwide fully dedicated to AML/CFT compliance, detection and investigation work, as well as economic sanctions compliance. Today, a little over half of these people are dedicated to finding customers or activity that is suspicious. The remainder—and the vast majority of employees dedicated to these efforts in the business and operations teams that support the firm's AML program—are devoted to perfecting policies and procedures; conducting quality assurance over data and processes; documenting, explaining, and governing decisions taken relating to their compliance program; and managing the testing, auditing, and examinations of their program and systems.

By point of reference, the more than 800 is greater than the combined authorized full-time employees in Treasury's Office of Terrorism and Financial Intelligence and the Financial Crimes Enforcement Network.

Baer urged officials and financial institutions to consider the potential for the use of AI and machine learning to improve AML systems.

"AI does not search for typologies but rather mines data to detect anomalies," he explained. "It gets progressively smarter; it would not be easily evaded; and different banks with different profiles would end up producing different outcomes. The current system is not progressing from typology to anomaly, however, because there has been no signal whatsoever from the regulatory agencies

"AI does not search for typologies but rather mines data to detect anomalies. It gets progressively smarter; it would not be easily evaded; and different banks with different profiles would end up producing different outcomes."

Greg Baer, President, Clearing House Association

that dollars can be shifted from the existing, rules-based system to a better one."

But there are obstacles, Baer said. Artificial intelligence strategies require feedback loops, which do not exist in the current system. In addition, there are barriers to cross-border information sharing of suspicious activity for global financial institutions.

Baer also encouraged the exchange of AML/CFT information between the government and the private sector as well as between and among financial institutions. He applauded the FinCEN Exchange program, launched on December 4, in which FinCEN will meet with law enforcement and financial institutions every six to eight weeks to exchange information on priority illicit finance threats, including targeted information and broader typologies. This is intended to enable financial institutions to better identify risks and focus on high-priority issues.

"Such sharing not only makes financial institutions' programs more effective and efficient, it assists in focusing their resources on important matters," he said.

"Strong public-private partnerships and two-way information sharing is a crucial component of our efforts to combat the sophisticated money laundering methods and evolving threats we face today," said Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence.

Private-sector participation in FinCEN Exchange is strictly voluntary, and the program does not introduce any new regulatory requirements.

"Improving information sharing is not limited to the exchange of information between the public and private sectors. We welcome efforts by financial institutions to share information with each other," Mandelker said.

"We know that some banks have started forming consortia to share information more dynamically under Section 314(b) of the USA PATRIOT Act," he added. "By working together, these groups of financial institutions have provided substantial insight into illicit finance threats that otherwise may be invisible to a single institution. We are highly encouraged by the private sector's willingness to engage in this type of exchange, and we appreciate the amount of time and effort that is going into these projects."

Heather Lowe is legal counsel and director of government affairs at Global Financial Integrity, an organization dedicated to curtail illicit financial flows. She supports greater information sharing among banks and with the government, but injects a note of caution.

"While we generally support greater sharing of information in the AML area, it must be done with appropriate privacy safeguards," she says. "Where it may result in a person being denied banking services at all, there must be a system for redress for people to be able to restore that access if they can demonstrate that they are involved in legitimate activity."

"Transferring raw banking data from banks to FinCEN to analyze (with appropriate privacy safeguards) is not a bad idea," Lowe added. "However, it is essential that we do not absolve banks of the responsibility to carry out their own analysis as well, which they have the ability to review within the context of the additional client information that they have, because they are the gatekeepers to the financial system. The federal government cannot do this alone." ■

War on AML imperative

Another imperative in the fight against money laundering is ensuring that boards of directors also make the crime more of a priority.

Even though financial institutions are aware of risks related to money-laundering and sanctions-related investigations, many of them may be "de-risking"—disassociating themselves, perhaps needlessly, from otherwise-profitable businesses and relationships,

That's according to a survey of financial services executives and boards of 361 financial institutions around the world from AlixPartners, a global business advisory firm. At the same time, a significant number lack both adequate AML and sanctions compliance budgets and training for their boards.

According to the survey, nearly two-thirds of respondents have experienced de-risking in one form or another—a trend that could actually increase institutions' AML and sanctions risks, as customers seek other avenues for conducting their business with the institution, such as creating "nested" relationships in the case of correspondent banks. This could be even more difficult to detect and subsequently report potentially suspicious activity and/or sanctions violations.

Meanwhile, 32 percent of respondents say they consider the AML and sanctions-compliance budgets at their firms to be "inadequate" or "severely inadequate." And, in what the survey's authors say may be a sign that an understanding of AML and sanctions risks hasn't fully permeated the upper reaches of many financial institutions, 20 percent of respondents say their board is not receiving AML and sanctions training and regular briefings, despite many new compliance standards having recently been implemented around the world.

"As with all matters important to a financial institution, success in AML and sanctions preparation hinges on having clear support from senior management and the board," says Sven Stumbauer, a managing director in the financial advisory services practice at AlixPartners. "If you want to create a culture of compliance, the tone and expectations need to be set at the top and supported by ongoing education and training."

According to the survey, one way that institutions are continuing to step up their compliance efforts is through technology; with a majority of respondents (54 percent) saying AML and sanctions compliance monitoring systems are their top investment areas for the next 12 to 24 months.

"Robust IT systems and the relevant input information are a critical component of AML and sanctions compliance," added Stumbauer. "Institutions feel having the right kind of tools is imperative to detecting and reporting on suspicious activity or potential sanctions breaches, which is showing no signs of slowing. However, not all institutions believe their current systems are adequate or sufficiently fine-tuned."

The survey also found that 92 percent of respondents saying their firms have a formal AML and sanctions-compliance program in place. However, 35 percent say their firms don't perform independent annual reviews or benchmarking reviews of these programs.

—Joe Mont

What casinos, bitcoin tell us about money laundering

Joe Mont looks at recent speeches from the director of the Treasury Department's Financial Crimes Enforcement Network who discussed money laundering issues for—and the need for cooperation from—casinos.

During a pair of recent speeches, Kenneth Blanco, director of the Treasury Department's Financial Crimes Enforcement Network, discussed money laundering issues for—and the need for cooperation from—casinos. Another topic: the regulatory perils of virtual currencies.

"I believe casinos are good and important partners that have made significant progress in recent years with respect to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). There are, of course, as in most industries, areas for improvement," Blanco said at the 11th Annual Las Vegas Anti-Money Laundering Conference and Expo.

He stressed that FinCEN is able "to do important things with the data that casinos and other financial institutions provide every day."

"As many of you know, Bank Secrecy Act data is one of the first lines of defense in our fight against all kinds of crime and bad acts, including terrorism," Blanco said.

Nearly 500 federal, state, and local law enforcement and regulatory agencies have access to FinCEN's database of BSA records, he explained. Within these agencies, there are an estimated 11,000 active users of BSA data. This includes 149 Suspicious Activity Report review teams located all around the country, covering all 94 federal judicial districts—including one in each state, Washington D.C., and Puerto Rico.

Law enforcement, regulatory users, and FinCEN analysts have made more than 10 million queries of the BSA database over the past five years. More than 20 percent of FBI investigations utilize BSA data, and for some types of crime, including organized crime, that number is nearly 60 percent.

FinCEN receives nearly 1,900 SARs related to terrorist financing each year. "Keep in mind that those SARs are only the ones that the financial institutions filing the reports have identified as potentially relating to terrorism," Blanco said. "We then take those and connect them to other SARs and other BSA information, which can generate further leads."

He added that of 97 recent domestic terrorism cases reviewed by FinCEN, 25 of them had BSA reporting prior to a person's arrest.

Blanco gave specific instances of BSA-related reporting aiding enforcement actions.

Reporting by casinos helped the Internal Revenue Service and several other federal agencies working together to combat Mexican kleptocracy involving senior political figures and the illicit use of the U.S. financial system to launder bribe payments received from Mexican drug cartels.

Financial data, including multiple BSA records filed by two separate casinos, played a critical role in this investigation by initially bringing the criminal activity to the attention of investigators and identifying numerous co-conspirators and previously undiscovered accounts and transactions from Mexico to the United States.

As a result, assets totaling more than $80 million were seized, including residential and commercial real estate, financial accounts, currency, gold coins, jewelry, vehicles, and aircraft. In addition, the subjects of the investigation were charged with various financial crimes, including money laundering, bank fraud, wire fraud, operating unlicensed money services businesses, loan fraud, racketeering, and others.

"BSA reports filed by casinos ultimately played a role in a case involving an international fraud network and a kleptocracy investigation. The reports your casinos file matter," Blanco said. "They are valuable. They make a difference.

"While BSA data may not assist with specific investigations, that does not mean that it is any less valuable," he added. "FinCEN and law enforcement officials regularly analyze and work with the data to connect networks, to understand trends and typologies, and to develop red flags which assist financial institutions and law enforcement. When we combine this data with open source data and information from law enforcement… we can map out connections that we would not otherwise see or even know about. These networks would otherwise remain in the shadows."

Part of getting better and doing more includes providing financial institutions better and more consistent feedback on how investigators use BSA data, so they understand our priorities and how to use their resources more efficiently and in a more targeted and focused manner, Blanco explained.

Reporting by a casino in Argentina, for example, helped piece together an investigation into a transnational criminal organization linked to Hezbollah and its global terror network.

"It is critical that casinos utilize the information they have on an enterprise-wide basis and ensure it gets into the hands of the right people in your compliance departments," Blanco said. "We know the kind of significant information that casinos are able to develop on gaming customers. This information is extraordinary and relevant and already used by casinos for a variety of marketing and other business purposes. But this information can, and should, be used by your compliance personnel as they monitor customers for suspicious activity. Information developed by your security

departments for combating and preventing fraud should also be shared with compliance personnel."

Larger casinos may have multiple affiliated casinos that could benefit from the sharing of information across the organization, Blanco said.

To facilitate the sharing of information across components of a gaming enterprise, FinCEN issued guidance in January 2017 clearly stating that under the BSA and its implementing regulations, a casino that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with each office or other place of business located within the United States of either the casino itself or a parent or affiliate of the casino, he explained.

Blanco gave another example of BSA disclosures in action. In May 2018, FinCEN settled a case against Artichoke Joe's Casino, a card club in San Bruno, Calif. The settlement included a $5 million civil penalty with an additional $3 million suspended pending the completion of several remedial undertakings for willful violations of the BSA that occurred over an eight-year period.

FinCEN learned employees—including senior managers—observed loan sharking and other illicit activity taking place on the gaming floor that was not reported.

There was also a failure to address risks associated with some of the gaming practices offered. Artichoke Joe's offered a practice called "backline betting," which enabled players who were not at the gaming table to bet on activity at the table. According to FinCEN, the casino had no procedures in place to identify participants in backline betting, despite previous guidance on the topic.

Another lesson learned from the Artichoke Joe's case is the importance of ensuring that gaming establishments address some of the "basic" requirements outlined in the regulations, Blanco said.

For years, he said, Artichoke Joe's operated under a written compliance program riddled with blank passages or placeholder language. It was never completed. The casino conducted its first independent test in August 2011, following the execution of search warrants and arrests by state and federal officials.

"Neglecting fundamental issues such as the need for independent testing heightens the risk that your gaming establishment will be exploited by criminal actors," Blanco said.

With these enforcement actions as a backdrop, FinCEN is encouraging increased information sharing through its voluntary 314(b) Program

"Just like other FinCEN-regulated financial institutions, casinos can share information with one another and with other regulated financial institutions, such as banks, under Section 314(b) of the USA PATRIOT Act," he explained. "Information sharing under 314(b) can be useful in a variety of ways. It may be particularly useful in helping casinos gain a better understanding of their customers' sources of funds."

"As we have noted on multiple occasions, information on source of funds is critical to ensuring compliance with your SAR filing obligations," he added. "For example, if you have a large foreign clientele, sharing information with other institutions can help you address and report concerns related to foreign corruption."

"Given the clear and significant value of this information sharing," Blanco said that he is concerned the number of 314(b) registrations for casinos has decreased since 2017.

At one point, there were more than 200 casinos registered to share information, but today that number stands at 183. And with more than 6,400 financial institutions participating in the 314(b) program, this means casinos make up only 2 percent of registrants.

"This trend is surprising to me," Blanco said. "This is an area that we want to work with you on, to make sure that we communicate clearly the benefits and importance of the 314(b) program so that all of you can better understand its importance. ... The program is voluntary, but FinCEN strongly encourages all financial institutions, including casinos, to participate. Remember that participation means you are able to share with other financial institutions—not just other casinos and card clubs.

Speaking at a legal technology conference in Chicago a few days earlier, Blanco discussed FinCEN's approach to virtual currency and emerging technology.

"Innovation in financial services can be a great thing—providing customers greater access to an array of financial services and at faster speeds than ever before," he said. "However, as industry evolves and adopts these new technologies, we also must be cognizant that financial crime evolves right along with it, or indeed sometimes because of it, creating opportunities for criminals and bad actors, including terrorists and rogue states."

Virtual currency, he said, presents numerous concerns.

"Major money services businesses are looking at how to incorporate blockchain payments to expedite remittances to locations around the world," he said. "But like any payment system or medium of exchange, virtual currency has the potential to be exploited for money laundering and other illicit finance."

In 2011, FinCEN issued a final rule amending definitions and other regulations relating to money services businesses to provide that money transmission covers the acceptance and transmission of value that substitutes for currency. Virtual currency is such a substitute and is covered by that regulation. Since then, FinCEN has issued several administrative rulings clarifying how this affects different business models in the virtual currency space.

FinCEN's March 2013 guidance indicates that rules apply to all transactions involving money transmission—including the acceptance and transmission of value that substitutes for currency, which includes virtual currency.

Businesses providing anonymizing services (commonly called "mixers" or "tumblers"), which seek to conceal the source of the transmission of virtual currency, are money transmitters when they accept and transmit convertible virtual currency, and, therefore, have regulatory obligations under the BSA.

"In short, individuals and entities engaged in the business of accepting and transmitting physical currency or convertible virtual currency from one person to another or to another location are money transmitters subject to the AML/CFT requirements of the BSA and its implementing regulations," Blanco said.

To comply with these obligations, virtual currency money transmitters are required to: register with FinCEN as a money services business; develop, implement, and maintain an AML program designed to prevent the MSB from being used to facilitate money laundering and terrorist finance; and establish recordkeeping, and reporting measures, including filing SARs and Currency Transaction Reports (CTRs).

"A strong culture of compliance should be part of building your operations from the ground up, and you can expect that we will identify where this is not taking place and take appropriate action."

Kenneth Blanco, Director, Financial Crimes Enforcement Network, Treasury Department

"We would also expect financial institutions adopting new FinTech to assess and understand whether the new financial products and services may be vulnerable to exploitation for financial crime; and whether this financial service activity has AML/CFT obligations under FinCEN's regulations," Blanco said.

He added: "Compliance does not begin because you may get caught, or because you are about to be discovered. That is not a culture that protects our national security, our country, and our families. It is not a culture we will tolerate. A strong culture of compliance should be part of building your operations from the ground up, and you can expect that we will identify where this is not taking place and take appropriate action." ■

Guidepost

FINTRAIL SOLUTIONS

OUT OF MANY, ONE?—THE FUTURE OF U.S. FINTECH REGULATION

NOT FOR THE FIRST TIME, THE FEDERAL GOVERNMENT AND STATES ARE AT ODDS OVER THE FUTURE REGULATION OF FINTECH.

An earlier version of this article was published in FinTechWeekly August 29, 2018. Authored by Julie Myers Wood and Gemma Rogers.

On July 31, 2018, the Office of the Comptroller of Currency (OCC) at the U.S. Department of the Treasury (DoT) announced it would begin accepting applications from FinTechs for special bank charters, which would allow them to operate nationally. But individual states and inter-state organizations are strongly opposed. The Conference of State Bank Supervisors (CSBS), which brought an unsuccessful lawsuit against the OCC last year to stop the charter being introduced, has declared that it is 'a regulatory train wreck in the making.'

The irony is that both sides of the debate want greater consistency. The key difference is determining who should drive the change. As this battle continues, how can U.S. FinTechs approach this complex regulatory landscape, protect themselves and their customers from financial crime, and change potential risks into competitive advantages?

No Single Framework

Part of the difficulties FinTechs face while navigating the U.S. regulatory environment are not only the different layers of government—state and federal—but also the lack of one single type of FinTech. Digital payments firms, for instance, are seen as money service bureaus (MSBs) under the federal Banking Security Act (BSA) and have to register both with the Financial Crime Enforcement Network (FinCEN) at the DoT, as well as gain a state license. Cryptocurrency exchanges are also considered MSBs, because they transmit funds, but initial coin offerings (ICOs), where a new cryptocurrency is offered in return for investment in the startup, is considered a form of security and is subject to the Securities Act and Securities Exchange Act, regulated by the Securities and Exchange Commission (SEC).

Meanwhile, the international inter-governmental body Financial Action Task Force (FATF), of which the United States is a member, has also issued guidelines related to FinTech, but they currently apply only to virtual currency payment products and services. Recently, FATF has promised to issue broader principles meant to unify the global FinTech world. The table below provides a simplified view of financial crime risks, regulations, and the FinTech sectors that might be affected.

FINTECH SECTOR	CURRENT FEDERAL REGULATIONS OF PRIMARY CONCERN PER SECTOR								STATE REGS
	ANTI-MONEY LAUNDERING (AML) & COUNTERING FINANCING OF TERRORISM (CFT)			FRAUD (CREDIT & SECURITIES)		SANCTIONS EVASION	TAX EVASION	ANTI-BRIBERY & CORRUPTION (ABC)	ALL RISKS, INCLUDING FINANCIAL CRIME
	Financial Crime Enforcement Network (FinCEN) Registration	Banking Security Act (BSA) AML/CFT & PATRIOT Act KYC Requirements	Financial Action Task Force (FATF)	Registration with Securities and Exchange Commission (SEC)	Registration with Consumer Financial Protection Bureau (CFPB); Federal Deposit Insurance Corporation (FDIC)	Subject to US Sanctions Laws, administered by Office of Foreign Assets Control (OFAC)	Subject to US Tax Code and the Foreign Account Tax Compliance Act (FATCA), administered to by the Internal Revenue Service (IRS)	Subject to Foreign Corrupt Practices Act (FCPA), administered by SEC and the Department of Justice	Licensing – requirements will vary by state
Digital Payments	✓	✓	✓	✗	✗	✓	✓	✓	✓
Mobile / Virtual Wallets	✓	✓	✓	✗	✗	✓	✓	✓	✓
Remittances	✓	✓	✓	✗	✗	✓	✓	✓	✓
Mobile Banking	✓	✓	✓	✗	✓	✓	✓	✓	✓
Cryptocurrency	✓	✓	✓	✗	✗	✓	✓	✓	✓
Exchanges	✓	✓	✓	✗	✗	✓	✓	✓	✓
Cryptocurrency ICOs	✓	✓	✓	✓	✗	✓	✓	✓	✓
P2P Lending	✓	✓	✓	✓	✓	✓	✓	✓	✓
Crowdfunding	✓	✓	✓	✓	✗	✓	✓	✓	✓
Robo-Investment Advisers	✗	✗	✗	✓	✗	✓	✓	✓	✓
Smart Financial Management	✗	✗	✗	✓	✗	✓	✓	✓	✓

What Do Both Sides Want?

First, the states are keen to see licensing for FinTechs remain in their hands, and there have been collective moves to increase alignment and streamlining across the states for all forms of non-bank financial activity. CSBS's 'Vision 2020' reinforces this with what it calls is "a series of initiatives…to modernize state regulation of non-banks, including financial technology firms." The program aims to ensure that by 2020, there will be an integrated state licensing and supervisory system across all 50 states. This includes the redesign of Nationwide Multistate Licensing System (NMLS), the core technology platform used by state bank regulators, the introduction of a Fintech Industry Advisory Panel, harmonization of state supervision, and education programs to improve bank and non-bank interaction.

According to the recent DoT report, 'Nonbank Financials, Fintech, and Innovation,' the federal government wishes to see financial innovation continue, but within a more consistent regulatory framework. The report suggests a range of possibilities, such as state alignment through 'model laws,' license harmonization, FinTech/Financial Service provider partnerships, as well as the OCC 'special bank' charter. Indeed, the OCC itself has said that the special charter is only one option, and it is conceivable that a hybrid approach might develop over time, through negotiation between the states and the federal government. All sides seem to want to get to the same destination, but have varying views about who should be in charge.

sector, there are plenty of positives in these developments. Variations in types of regulation between jurisdictions can create vulnerabilities in a system that can abet money launderers. Federal legislation apart, if one state has significantly less demanding requirements for company licensing than another, then it could become a portal through which criminal funds are most easily 'placed' in the financial system—stage one of the money laundering cycle. And from there, the funds can be 'layered'—sent through multiple accounts in the financial system (stage two)—before being 'integrated' into a seemingly legitimate account (stage three), quite possibly in a state with higher licensing requirements. If there is greater and more demanding standardization, and more consistent application of the standards, this should then help to reduce financial crime risk overall.

How should FinTechs respond?

However, it is important that FinTechs do not interpret this positive trend in the wrong way. Improved and consistent regulation can reduce some of the niches in which financial criminals can operate. However, it does not eliminate financial crime risk, because, as experience has shown, those who launder criminal funds, evade sanctions and tax, and finance terrorism, are amongst the most creative people in the world.

So rather than becoming caught up a traditional compliance 'tick box' culture, or following regulatory battles, FinTechs should focus first on the actual financial crime risks themselves. Regardless of the final outcome of the tug of war between the states and the federal government, FinTechs must consider how to manage their risks in this area, in the best interests of themselves and their clients. This isn't just good for risk management and compliance—it is also good for business.

FinTech firms should consider a simple four step approach:

1. Undertake a financial crime risk assessment. This is essential to knowing your key vulnerabilities and then being able to measure your efforts to reduce them over time. This requires challenging assumptions, testing vulnerabilities, and working in detail to understand the precise extent and nature of money laundering and other risks to which it could be exposed.

2. Understand financial crime typologies. Make use of available typologies studies related to certain offences, to understand potential exposure and assess whether any unknown risks do in fact exist. Given the anonymous character of many transactions on online platforms, FinTechs should pay special attention to the risks from different types of fraud, such as synthetic identity fraud.

3. Tailored systems. Seek to build systems and processes that are specifically designed for the risks FinTechs are likely to face. For example, although all financial institutions are subject to U.S. sanctions laws, providers involved in cross-border transactions should give higher priority to screening for potential evasion. A risk focused approach is more likely to create a healthy and proactive compliance culture.

4. Create indicators and use data: FinTechs should leverage the skill they have in utilizing data to decipher indicators of specific money laundering risks. They should continue using these indicators and supporting data as key performance indicators on a regular and scheduled basis. This is invaluable for managing risk and makes the process of future conversations with auditors and regulators considerably easier.

Understanding and implementing this process is key to stopping financial crime in its tracks and helping transform risks into opportunities.

ABOUT THE AUTHORS

JULIE MYERS WOOD
CHIEF EXECUTIVE OFFICER
GUIDEPOST SOLUTIONS

Julie Myers Wood is the chief executive officer of Guidepost Solutions. She focuses on regulatory compliance and investigative work and has significant experience as a monitor on issues related to sanctions and anti-money laundering for global entities. Her experience includes assisting FinTech companies with developing and creating compliance and security protocols in the context of a changing and complex regulatory environment. Prior to joining the private sector, Ms. Wood served as Head of Immigration and Customs Enforcement for the U.S. Department of Homeland Security leading its largest investigative component and the second largest investigative agency in the federal government. She can be reached by email at jwood@guidepostsoltuions.com.

GEMMA ROGERS
CO-FOUNDER
FINTRAIL LTD

Gemma Rogers is the co-founder of FINTRAIL LTD., a financial technology compliance consulting firm. She has a passion for changing the terms of debate around financial crime risk management, debunking the lethargic tick-box concepts of old and focusing on intelligent, inclusive and business-focused solutions. Drawing on her wealth of experience across disruptive services, international banking and the public sector, Gemma brings clients deep domain knowledge of financial crime risks, as well as an ability to execute intelligent frameworks across both emerging platforms and established financial services. She can be reached by email at gemma.rogers@fintrailsolutions.com.

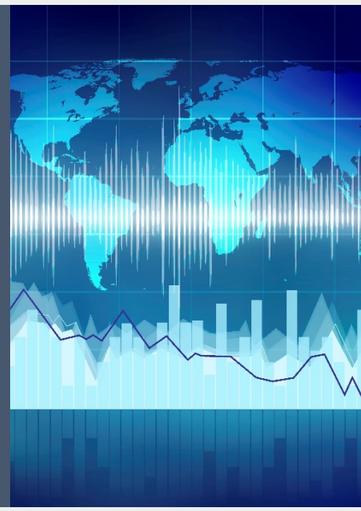
ABOUT GUIDEPOST SOLUTIONS

In a world where change is certain, experience is the best protection. Guidepost Solutions offers global investigations, compliance, monitoring, and security and technology consulting solutions for clients in a wide range of industries. Our expert team provides leadership and strategic guidance to address critical client needs across the globe.

Experience guides us. Solutions define us. www.guidepostsolutions.com

ABOUT FINTRAIL SOLUTIONS

Guidepost Solutions LLC, a global leader in compliance, investigations, and security consulting, in conjunction with financial technology compliance consulting firm FINTRAIL LTD., launched FINTRAIL Solutions LLC, a financial crime consultancy company to offer North American FinTech and RegTech firms with specialized services to manage their risks and navigate the uncertainty of future regulations for themselves and their clients.
www.fintrailsolutions.com



AML risk multiplies, as cryptocurrency arrives

As mainstream firms dip their toes into cryptocurrency, they are discovering an evolving world of money laundering controls and sanctions restrictions, writes **Joe Mont**.

By now, our readers—like most of By now our readers—like most of the world—likely divide into two camps: those with a fanatical zeal for the financial innovations (and potential profits) created by virtual currencies and those who see a modern version of "Tulip Mania," poised to bubble and pop.

Regulators around the world are increasingly falling into the latter camp, especially as the trend starts to slowly go mainstream, fearing fraud and criminal activities.

Christine Lagarde, managing director of the International Monetary Fund, is among those to recently cite the threat of both money laundering and sanctions evasion for cryptocurrencies.

"We need to define the legal status of a virtual currency, or digital token," she wrote on an IMF blog. "We need to combat money laundering and terrorist financing by figuring out how best to perform customer due diligence on virtual currency transfers. The regulatory challenges are just emerging. For instance, cryptocurrencies like Bitcoin can be used to make anonymous cross-border transfers—which increases the risk of money laundering and terrorist financing."

The big question is how regulators can, or should, regulate virtual currencies and Initial Coin Offerings (ICOs), a public offering of sorts to raise money for a new cryptocurrency.

"It is difficult for U.S. regulators to regulate cryptocurrency projects for several reasons," says Jeffrey Alberts, partner and head of the white-collar defense and Investigations practice at law firm Pryor Cashman. He previously held a post with the U.S. Attorney's Office for the Southern District of New York.

"First, the decentralized organization of many such projects often results in the absence of any formal corporate entity on which the regulators can focus their attention," he explains. Many participants are located outside the United States and, "many of the entities are so small that they do not have the infrastructure to respond to regulatory inquiries and attempts at oversight."

These problems haven't stopped government agencies from inching toward a regulatory regime. Guidance and enforcement actions have focused on investor fraud, Ponzi cons, and get-rich-quick schemes by penny stocks and other entities.

"We even see cases where there are celebrities hawking these things," says Eric Sohn, director of business product at Dow Jones Risk & Compliance. "I even saw an advertisement the other day that suggested you should invest your retirement money—your 401k money—in ICOs, or taking out a home equity loan to invest in bitcoin. That is pretty scary given how relatively threadbare most ICOs are."

As virtual currencies and ICOs gradually enter the mainstream, money laundering is poised to take its place alongside fraud as a top concern.

"ICOs are really good money laundering vehicles," Sohn says. "They are similar to what we call a transit account. You open up an ICO. Then you get the people who are collecting your drug money across the United States to buy those coins. Then, you abscond with that money, look like any other failed business, and open another new line in another country. A lot of countries haven't started doing any kind of regulation regarding virtual currencies and ICOs. The U.S. is very much the exception."

Business debate risk, seek cautious adoption

Concerns of this sort are made all the more concerning as mainstream companies choose to either join the fray or retreat from the inherent risk. The latter group is starting to lament virtual currencies in their 10-K itemizations of risk factors.

Among them is Cardtronics, the world's largest non-bank ATM operator, as well as investment banking giant Goldman Sachs. Bank of America, which once dabbled with patents for a cryptocurrency exchange, wrote in its 10-K: "The widespread adoption of new technologies, including internet services, cryptocurrencies, and payment systems, could require substantial expenditures to modify or adapt our existing products and services."

Companies that have decided to block advertising related to ICOs and virtual currency include Google, Facebook, and Twitter (despite its founder's exhortation that Bitcoin might eventually replace traditional fiat currencies).

JPMorgan Chase, Bank of America, and Citigroup have separately announced that they will no longer allow the purchase of Bitcoin and other virtual currencies using credit cards.

Other entities, moving beyond the inherent risks, are embracing the new technology. Overstock.com was the first major online retailer to accept bitcoin payments. The payment technology company Square now allows Bitcoin trading for its users. PayPal added bitcoin to the list of currencies it will accept.

Shopify, a Canadian e-commerce company and cloud-based platform for online stores and retail point-of-sale systems, now gives merchants the option of bitcoin payments. Microsoft similarly allows bitcoin as a currency to purchase games, movies, and apps in the Windows and Xbox stores.

One-time photography giant Kodak recently announced the launch of the KODAKOne image rights management platform, "a photo-centric crypto-currency." Chanticleer Holdings, a company that owns a minority stake in Hooters (and has a portfolio that includes other chain restaurants) moved its customer loyalty programs to blockchain, touting that "eating a burger is now a way to mine for cryptocoins."

The Chicago Board Options Exchange jumped on the bandwagon and became the first exchange to allow bitcoin futures trading. CME Group followed suit and Nasdaq is said to be considering its options in the space.

Stressing sanctions screening

A notable regulatory move into the world of cryptocurrencies comes from the Treasury Department's Office of Foreign Assets Control. On March 19, it released a "frequently asked questions" document

that may serve as a prelude to including digital currency addresses on its Specially Designated Nationals list of blocked persons and companies.

OFAC compliance obligations are the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency, OFAC emphasized.

"Persons including technology companies, administrators, exchangers, and users of digital currencies, and other payment processors should develop a tailored, risk-based compliance program, which generally should include sanctions list screening and other appropriate measures," OFAC adds. "An adequate compliance solution will depend on a variety of factors, including the type of business involved. There is no single compliance program or solution suitable for every circumstance."

The agency added that it "may add digital currency addresses to the SDN List to alert the public of specific digital currency identifiers associated with a blocked person."

"Parties who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN and hold such property should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details," it wrote.

Petro is a sovereign cryptocurrency issued by Venezuela and backed by oil assets. In March, President Trump issued an order banning U.S. purchases of the virtual currency.

The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) is also on the case, stressing money-laundering concerns.

"Probably the most significant question you will need to answer in relation to your anti-money laundering obligations as you prepare to undertake a token sale is whether your sale amounts to 'money transmitting' under federal law," says O'Melveny attorney Laurel Loomis Rimon.

Money transmitting regulations apply to virtual currencies and ICOs, according to guidance from FinCEN, she points out. Operating a money transmitting business without meeting Bank Secrecy Act requirements could subject both your business and the individuals involved in it to civil and criminal penalties.

Rimon was previously the top lawyer for the Office of the Inspector General at the U.S. Department of Homeland Security. In addition, she served as the assistant deputy enforcement director at the Consumer Financial Protection Bureau and held senior positions at the Department of Justice, including in the Asset Forfeiture and Money Laundering Section.

While an assistant United States attorney in the District of Columbia, Rimon successfully handled the money laundering and money transmitting prosecution of the "E-gold" enterprise, one of the earliest digital currencies. It allowed users to open an account that exchanged cash for online commerce credits that were denoted in grams of gold and accepted by other e-gold accounts. For Rimon, the modern cryptocurency gold rush prompts somewhat of a déjà vu feeling.

"I see a lot of similarities and many of the same challenges are out there," Rimon says. "The activity (at E-gold) was money transmitting and that was clear in the government's point of view [even before FinCEN codified the issue], but a lot of the issues that are of concern now are really the same. Avoiding money laundering is still a challenge. You have so many people rushing into this market right now and developing products that don't have effective anti-money laundering programs."

"The criminal element is very opportunistic and with E-gold, with no controls in place, they flooded into the platform. What you saw was a large portion of the transactions being conducted by people engaged in investment fraud, Ponzi schemes, child pornography, and credit card fraud."

A key attraction of modern cryptocurrency offerings is their perceived anonymity. "You have a more advanced technology that is not necessarily anonymous, but tracing can be a challenge," Rimon says. Like E-gold, many modern platforms invest little time or effort in verification. Although the former service required a name, there was no shortage of those claiming to be Mickey Mouse and Donald Duck.

Things are only slightly better today. "I see a lot of these offerings are doing some 'Know Your Customer,' but whether it is enough or not is still an open question," Rimon says.

Even a legitimate product or offering can still be compromised, despite the warnings and lessons of E-gold.

"A lot of the focus right now is on being compliant, with a lot of consternation over all of the regulators that have jumped into this and overlapping jurisdictions," Rimon says. "Nobody is quite sure: Are we a security, or a money services business? Are we both? There is a lack of clarity on the government's side, and the developers are really scrambling to try to figure out what they need to do. But put all that regulatory stuff aside, even though it matters, you need to make sure that your platform doesn't facilitate money laundering. That isn't just a regulatory problem. It is a criminal problem."

A recent development, Rimon says, is that those in the virtual currency space are seeking third parties that can provide KYC and anti-money laundering services, "but they may be relying on someone else who hasn't fully built out their platform and product as thoroughly as they should have."

"But that's who they look to because that's who they trust; they are looking for other developers like them who speak the same language," she says. When it comes to sanctions compliance, however, OFAC has strict liability. "You can say you outsourced it to someone who said they did the screening, but you are still liable."

Money laundering carries a similar gravity. "When you look at the Silicon Valley atmosphere, there may be a reluctance to go to what might be considered 'your parent's AML program,' but it is something that takes some time and sophistication," Rimon says, comparing the situation to pressures forcing banks to de-risk. "The regulators have really pushed the banks to push down to their customers the development of AML programs and other compliance programs."

There are various red flags that can warn of money laundering risks.

"The key is to establish what is the pattern for your particular customer base. When you see anything that is different from what the routine pattern is, then you investigate that when it pops up," Rimon says.

Another warning sign includes transactions structured to evade a $10,000 threshold, the amount that requires banks to file Suspicious Activity Reports.

These enterprises need to determine if they fall under the criteria demanding they register as a money services business. FinCEN has stated that, in its view, Initial Coin Offerings will be treated as money transmitting firms. As such, they must register as a money transmitting business within 180 days from the date the organization was established.

As money transmitters, these organizations must comply with both federal law (notably the Bank Secrecy Act and related recordkeeping requirements) on top of regulations imposed by every state in which they conduct business. On the federal front, they will be required to establish a formal AML program with written policies and procedures, training programs, a designated AML compliance officer, and independent monitoring of the program.

A challenge for these cutting-edge AML programs is customer identification.

"People use these keys, long chains of letters and numbers, and you can't quickly identify who that is, which is the attraction for a lot of users," Rimon says. "But for conventional businesses, the traceability is a sea change. If law enforcement comes to them and asks for a download of all their transactions, they are used to being asked to do that with some identification of their customers. Now they can't." ■

EU proposes new money laundering rules

The European Commission wants to strengthen supervision over banks and other financial institutions to toughen up its fight against money laundering and terrorist financing after admitting present measures have "failed all too often." **Neil Hodge** reports.

The European Commission wants to strengthen supervision over banks and other financial institutions to toughen up its fight against money laundering and terrorist financing after admitting that present measures have "failed all too often."

The EU has proposed giving the European Banking Authority, the bloc's supervisory body for financial services, a powerful new mandate to monitor what firms are doing to tackle money laundering.

These powers include asking national regulators to investigate potential material breaches and to impose sanctions where necessary. If regulators fail to act, the EBA can override them and tackle individual banks for their failings directly.

Other, more general, measures include enhancing the quality of supervision through common standards, periodic reviews of national supervisory authorities and risk-assessments, as well as improving information collecting and data sharing between regulators, using the EBA as a "data hub." The Commission also wants better cooperation with non-EU countries on cross-border cases and to establish a new permanent committee that brings national regulators together.

The proposals, which must be agreed by member states and the European parliament, would be fast-tracked by amending existing legislation.

In his State of the Union address on 12 September, Commission President Jean-Claude Juncker said: "Europeans expect a Union that protects them. Today, we propose measures to allow us to fight money laundering more effectively across borders."

Europe likes to think it has the strongest regulations in the world to prevent money laundering: the EU's fourth and fifth Anti-Money Laundering Directives have both come into force in the past two years.

Despite these efforts, however, the Commission accepts that the rules "are not always supervised and enforced with the same high standards everywhere across the EU" and that "the system is as strong as its weakest link."

Recent cases have urged a rethink about how closely EU banks need to be monitored, especially in light of the collapse of ABLV Bank in Latvia and the freezing of assets at Pilatus Bank in Malta following allegations of sanctions busting by its Iranian owner.

Investigations such as the Panama Papers and the Global Laundromat series, which revealed the movement of $21 billion in dirty funds from Russia, also underline how poor supervision by member states and a lack of cross-border cooperation between law enforcement agencies is allowing money to flow from countries with high levels of corruption into Europe.

And the September €775 million (U.S. $905 million) settlement by Dutch Bank ING for money laundering offences, coupled with reports that Danske Bank allowed up to $150 billion in dirty money to flow through its Estonian operations, have also done little to help Europe's reputation as being a "world leader."

In a memo, the Commission lays the blame for anti-money laundering failings on three factors: delayed and insufficient supervisory actions to tackle weaknesses in financial institutions' anti-money laundering risk management; a lack of coordination and information sharing between national supervisors and regulators; and a lack of cooperation with countries outside of the EU to tackle the problem globally.

The situation has led Commission Vice President Valdis Dombrovskis to concede that "anti-money laundering supervision has failed all too often in the EU." ■

> "Europeans expect a Union that protects them. Today, we propose measures to allow us to fight money laundering more effectively across borders."
>
> Jean-Claude Juncker, President, European Commission

What the EU has done to curb money laundering

The EU has taken the threat of money laundering seriously over the past few years: the fourth Anti-Money Laundering Directive came into force in June 2017, and the fifth version of the rules must be embedded in all EU member states by January 2020.

Both directives are designed to strengthen the EU's regulatory framework, as well as promote and improve cooperation between anti-money laundering and prudential supervisors.

Yet recent cases such as ING and Danske Bank suggest that the EU is still as big a haven for dirty money as it ever was, and that the directives are only as useful as member states are prepared to enforce them, regulators are prepared to cooperate and share information, and banks are willing to follow the rules.

In May, the European Commission set up a working group bringing together the European Supervisory Authorities, the European Central Bank, and the chair of the Anti-Money Laundering Committee, to reflect on possible actions to ensure seamless cooperation between anti-money laundering and prudential supervisors in the European Union.

Indeed, money laundering has loomed large as a key issue for the EU to tackle in recent, high-level correspondence.

The Franco-German Meseberg declaration and roadmap issued on 19 June 2018 by the French and German leaders to reinvigorate greater EU cooperation highlights money laundering as a concern, as does a letter sent by Mario Centeno, president of the Eurogroup (the EU's committee of ministers aimed at discussing issues pertinent to the single currency) to the President of the European Council Donald Tusk on 25 June 2018..

—Neil Hodge

Mexico's financial services sector lax in AML controls

Politically exposed persons, the identification of beneficial ownership, and suspicious transactions all continue to bedevil Mexican banking efforts to combat money laundering and terrorism financing. **Jaclyn Jaeger** has more.

Financial institutions in Mexico did not make the honor roll this year in the country's latest report card on anti-money laundering and counter-terrorism financing efforts, which addressed serious weaknesses in the way banks assess and manage such risks.

The recently released 236-page "Mutual Evaluation Report" on Mexico was conducted by the Financial Action Task Force (FATF), an independent, inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. For the first time since 2008, FATF assessed Mexico's overall level of compliance with the FATF's 40 anti-money laundering and counter-terrorism financing (AML/CTF) recommendations, recognized globally as a gold standard.

Although the FATF noted that Mexico has a "mature AML/CFT regime, with a correspondingly well-developed legal and institutional framework," it also discussed several risks that have not yet been fully addressed by financial institutions. These risks concern customer profiling; the identification and risk classification of Politically Exposed Persons (PEPs); the identification of beneficial owners; and the quality of suspicious transaction reports.

This article explores some of those key risks, as well as opportunities for improvement, identified in the report:

Beneficial ownership risk. Many financial institutions seek to identify beneficial owners only to a limited extent, thwarting efforts to assess and manage money laundering and terrorism financing risks. Specifically, where financial institutions are required to identify beneficial owners—for legal persons categorized as high risk and natural persons—they "tend to over-rely on customers' self-declarations to determine who the beneficial owners are," the report stated.

Most legal persons are not categorized as high risk. In these situations, financial institutions need only obtain information on corporate customers' first layer of legal ownership, without seeking to reach the natural persons who ultimately own or control the entity.

"While some foreign banks, consistent with their group-wide policies, attempt to identify and verify the identity of the ultimate beneficial owners of legal persons regardless of their risk ratings, this is not the common practice of domestic FIs when dealing with legal persons not classified as high risk," the report stated. The compliance lesson here is that compliance officers at financial institutions must dig deeper to identify the true beneficial owners to fully protect themselves from domestic and international money laundering and terrorist financing threats.

"This issue, like many others raised in the FATF Report, is not unique to Mexico," says Juliana Carter, an associate at law firm Ballard Spahr. In fact, the U.S. Customer Due Diligence (CDD) regulations issued by the Financial Crimes Enforcement Network, and expected to take effect in May 2018 specifically allow covered financial institutions to rely upon customer declarations regarding beneficial owners. "This is because it can be supremely difficult for—and, thus, unfair to expect—financial institutions to vet the accuracy of a declaration that Person X 'really' is a beneficial owner of Entity Y," Carter says.

Mexican regulators must enact regulations like the CDD regulations in the United States before financial institutions can better identify their beneficial owners. Only then can financial institutions perform certain enhanced due diligence on potential clients in the case of red flags, or where declarations of beneficial ownership may not be accurate. "This due diligence could include checking available databases or public filings," Carter says.

Financial institutions don't need to look any further than HSBC to learn what can happen when a bank fails to maintain an effective AML program and conduct appropriate due diligence on foreign correspondent account holders. In 2012, HSBC paid a then-record fine of $1.2 billion for helping Mexican drug cartels launder $881 million in drug trafficking proceeds through HSBC Bank USA. As part of that resolution, HSBC entered into a five-year deferred prosecution agreement, which ended in December 2017.

Politically exposed persons (PEPs) risk. Many large financial institutions have developed methodologies to risk categorize customers based on multiple parameters, including type of customer; geographical region; products and services (e.g., involvement in international transactions or cash transactions). Nonetheless, these methodologies for risk categorizing customers "don't often appear sufficiently robust to reasonably reflect customer risk profiles," the FATF stated. This is evidenced by the fact that most financial institutions categorize PEPs as low risk, "reflecting their lack of understanding of money laundering threats of corruption," the report stated.

To identify domestic PEPs, many financial institutions rely on public databases where the names of certain senior officials at federal and state levels are published. Senior military officers, executives of state-owned companies, and officials at the municipal level, however, are not considered domestic PEPs and, thus, are not subject to the same level of transparency.

"As a result, the risks posed by domestic PEPs are being managed only to a limited extent," the report stated. The compliance and legal risk this poses, as described by the report, is that many financial institutions "do not obtain additional information on the origin and destination of funds and the intended nature of the business relationship or require manager's approval for establishing such relationships."

Examples of enhanced measures that regulations require financial institutions to perform on their high-risk customers include obtaining a manager's approval before establishing the business relationship; obtaining additional information on origin and/or destination of funds and the nature of business relationship; and reviewing their risk profiles at least twice a year.

Suspicious transaction reports (STRs). Another concern noted by the FATF concerns the quality of STRs. Specifically, the reporting by large financial institutions of "Unusual Transaction Reports" (UTRs), defined as transactions that may be related to money laundering or terrorist financing, is "not always as prompt as it should be," the report stated.

Financial institutions must use automated systems to monitor transactions and generate alerts as a first step for identifying UTR/STRs. Many financial institutions said UTRs/STRs are triggered most often by involvement of cash transactions; inconsistencies between a customer's profile and transactional behavior; and high-risk locations of the customer or transaction.

"In general, large banks' systems seem more robust, while the concerns are greater with respect to smaller banks and non-banks," the report stated. It added that these findings are consistent with observations made by the Comisión Nacional Bancaria y de Valores (CNBV), an independent agency responsible for supervising and regulating financial institutions in Mexico.

Specifically, the CNBV noted that some financial institutions generate either too few or too many alerts. In the former instance, reports that should have been reviewed were not flagged, whereas in

the latter instance, the quality and promptness of the analysis may have been compromised, according to the report.

The broader compliance lesson here: Some financial institutions "need to calibrate their systems to address this issue," the report suggested. Some need to improve on the quality of reporting, notably in relation to performing an adequate analysis and preventing the omission of critical information.

Again, Mexico is not alone in needing to improve its reporting; the United States similarly struggles with financial institutions filing too many reports or reports that are too opaque. "Typically, better training of employees leads to better suspicious activity reporting, the quality of which often turns on the report's level of detail," Carter says.

Laudable compliance practices

The report did not contain all bad news for financial institutions. For example, the FATF noted, many banks and brokerage firms appear to be implementing AML/CFT requirements regarding wire transfers beyond legal obligations. This is because banks generally consider wire transfers a high-risk product.

Among a few good risk management practices mentioned, some banks include the beneficiary's name and account number in cases where the bank is the ordering institution; screen transfers that lack information, including that on the beneficiary, in cases where the bank is the intermediary or beneficiary institution; and take actions upon detection of wire transfers that lack information—such as either rejecting transfers or requesting missing or invalid information from the institution from which the transfer was received.

Furthermore, the report stated, financial institutions generally pay special attention to business relationships and transactions with persons in high-risk jurisdictions. Some financial institutions and money services businesses—money remitters, exchange centers that only conduct currency exchange, and exchange houses that are authorized to carry out both remittance and currency exchange activities—indicated that they don't deal with persons, whether natural or legal, from countries for which the FATF calls for counter measures.

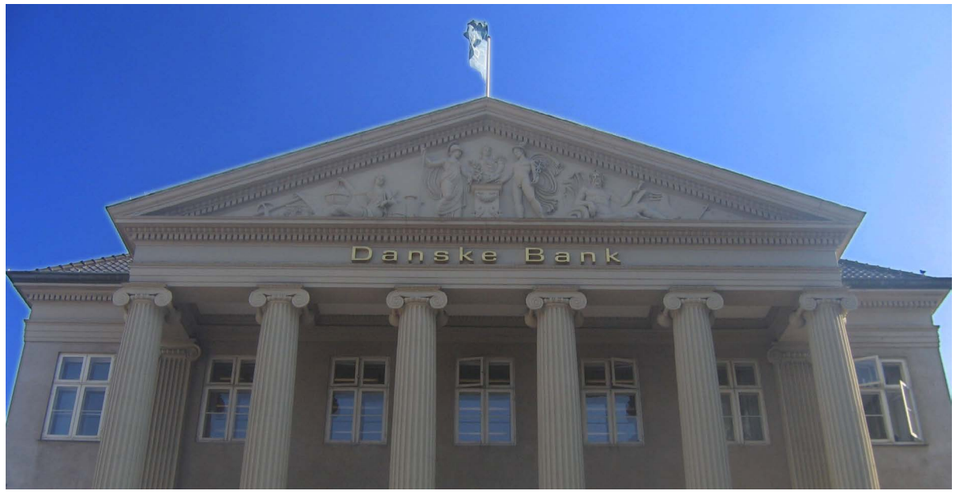
Additionally, some have also developed their own list of additional high-risk countries with which they do not conduct business. For transactions involving jurisdictions with strategic deficiencies identified by the FATF, financial institutions indicated that they "subject transactions involving these jurisdictions to enhanced monitoring by, for instance, developing special parameters or lowering the threshold for alerts to be generated," the report stated.

Compliance certifications

To further help improve and standardize AML/CFT knowledge and practice among compliance and audit professionals who render services to financial institutions, the CNBV implemented a program requiring that all compliance officers, as well as internal and external auditors, be certified through an examination process administered by the CNBV. The objective of this certification is to validate that compliance and audit professionals engaged in such activities possess the necessary knowledge on AML/CTF.

Certification must be renewed every five years. Since rolling out this requirement gradually since June 2015 across the various sectors supervised by CNBV, over 2000 certifications have been issued. The program is in the process of being extended to the insurance and pension fund sectors.

"The FATF's Mutual Evaluation Report on Mexico illustrates that successful AML procedures cannot occur in a vacuum, and that the success of FIs in implementing those procedures often depends upon context and the country in which they operate," Carter says. Although financial institutions can always work on improving their internal systems and processes, she says, "ultimately the adequacy of a particular country's AML system is a function of the relationship between industry and government, and the extent of the problems that a particular country may be facing." ■



Danske Bank CEO quits over AML failures

The chief executive of Denmark's biggest financial institution has resigned following the publication of a report that highlights large-scale money laundering in the bank's Estonian operations. **Neil Hodge** explores.

The chief executive of Denmark's biggest financial institution has resigned following the publication of a report that highlights large-scale money laundering in the bank's Estonian operations.

"It is clear that Danske Bank has failed to live up to its responsibility in the case of possible money laundering in Estonia. I deeply regret this," said Danske Bank CEO Thomas Borgen in a written statement released in September.

Danske has been under fire for failing to prevent dirty money from countries including Russia, Azerbaijan, and Moldova flowing through its Estonian branch, especially since the bank has had to revise initial estimates that less than €4 billion (U.S. $4.65 billion) was laundered, rather than the €100 billion (U.S. $116.8 billion) and counting that now seems more likely.

Even now, the bank is not able to provide an accurate estimate of the number of suspicious transactions made by non-resident customers in Estonia during the nine-year period between 2007-2015. A "significant part" of around €200 billion (U.S. $234 billion) in payments may be questionable. Of some 6,200 customers that have been identified as high risk, "almost all" have been reported to authorities.

Borgen is the second executive to stand down over the scandal. On 5 April, Lars Mørch, Danske Bank's executive responsible for its business and international banking units, resigned as a member of the executive

board over his failure to take warnings about possible money laundering offences in Estonia more seriously.

Anders Jorgensen, head of group compliance, resigned in July. Prior to Mørch taking the role, Borgen had been in charge of international banking for four years before becoming CEO. The first allegations of money laundering began on his watch. He had called the lack of controls in Estonia "deeply regrettable and completely unacceptable."

Danske commissioned law firm Bruun & Hjejle in autumn 2017 to investigate the allegations. Around 70 full-time investigators have examined close to 15,000 customers and 9.5 million payments as part of the investigation. Some 12,000 documents and more than 8 million emails have been searched. Investigators have also conducted more than 70 interviews with current and former bank employees and managers, including members of the executive board and members of the board of directors.

The firm's resulting Report on the Non-Resident Portfolio at Danske Bank's Estonian branch makes for uncomfortable reading for the bank's board.

It found that a series of major deficiencies in the bank's governance and control systems made it possible for criminals to use its Estonian branch for suspicious transactions from 2007, when it acquired Sampo Bank, right up until it terminated the customer portfolio in 2015. Danske had a large number of non-resident customers in Estonia (around 10,000, plus a further 5,000 with "non-resident characteristics") that it admits it should have never had and that these customers "carried out large volumes of transactions that should have never happened"—around €200 billion (U.S. $234 billion), in fact.

The investigation also found that only part of the suspicious customers and transactions were reported to the authorities as they should have been, and that in general, the Estonian branch had "insufficient focus" on the risk of money laundering. The report found that branch management was more concerned with procedures than with identifying actual risk and that the Estonian control functions did not have a satisfactory degree of independence from the Estonian organisation. Furthermore, the branch operated too independently from the rest of the group without adequate control or management focus and that it operated with its own culture and systems.

Worse still, investigators found evidence to suggest that employees in Estonia may have assisted or colluded with customers in circumventing money laundering controls. They also uncovered breaches at management level in several group functions. None of these incidences were identified or escalated for management or the board to act upon, and when action was eventually taken, it was too little, too late.

Several former and current employees (including managers), both at the Estonian branch and at group level, "did not fulfil their legal obligations," according to the report, and were disciplined through warnings, dismissals, and loss of bonus payments. Some have also been reported to the relevant authorities.

The board, the chairman, and the CEO, however, did not breach their own legal duties, the investigation found, and so escape censure—though not criticism.

In a statement, chairman Ole Andersen said: "The bank has clearly failed to live up to its responsibility in this matter."

"There is no doubt that the problems related to the Estonian branch were much bigger than anticipated when we initiated the investigations," said Andersen. "The findings of the investigations point to some very unacceptable and unpleasant matters at our Estonian branch, and they also point to the fact that a number of controls at the group level were inadequate in relation to Estonia."

Andersen added that the bank is "committed to using the report as a basis for continued learning and improvement" and said that "we will do everything it takes to ensure that we never find ourselves in the same situation again."

Danske closed down the portfolio of non-resident customers in Estonia in 2015 and has set up a pan-Baltic management team to strengthen governance and oversight in the Baltic States. Control functions in the region have been strengthened and processes and controls have been raised to group level to ensure the same level of risk management and control as in other parts of the organisation's network.

The bank has also reviewed how it combats financial crime and has quadrupled the number of full-time employees working in this area to 1,200. Its AML programme has been overhauled, and the bank has placed an emphasis on improving compliance knowledge and culture across the organisation, partly through a strong management focus and extensive mandatory training.

Other measures to improve governance include making senior managers and executive board members more directly accountable by including risk management and compliance in their performance agreements, and by strengthening its "three lines of defence" model and whistleblowing procedures.

Danske received its first whistleblowing report on possible money-laundering violations in its Estonian branch in December 2013, but despite follow ups by internal audit and compliance, management failed to take quick and decisive action.

The bank has also made a key appointment: Philippe Vollot, most recently head of anti-financial crime and group anti-money laundering officer at Deutsche Bank, starts as new group chief compliance officer on 1 December and will join the board.

As part of an effort to restore credibility, Danske says it will donate the gross income from its Estonian operations during the nine-year period—estimated to be about DKr1.5bn or U.S. $234 million—to an independent foundation that will be set up to combat international financial crime. ■

Europe struggles with money laundering

Despite the fact that AML is a priority of the European Union, Europe's banking sector cannot seem to get to grips with the rules and hundreds of pages of best practice that Brussels has produced in the past couple of years in the Fourth and Fifth Anti-Money Laundering Directives.

In May 2015, Sweden's financial services regulator fined Nordea, the region's largest lender, the maximum penalty allowed for lax anti-money laundering controls (SEK 50 million, or €4.8 million), while Handlesbanken, the country's second-biggest bank, was handed a SEK 35m (€3.3 million) fine for similar failings.

Danske Bank was fined DKr 12.5m (U.S. $2 million) last December by Danish authorities for violating anti-money laundering rules following an inspection in March 2015 (these were unrelated to the specific allegations in Estonia).

Meanwhile, in the Baltic States, Latvia's third-largest bank, ABLV, is in the process of liquidating itself after being accused by the United States of "institutionalised money laundering," and in March the European Central Bank pulled the plug on a small Estonian lender, Versobank, for money laundering offences.

In September, Dutch banking group ING admitted criminals had been able to launder money through its accounts for years and agreed to pay €775 million (U.S. $900 million) to settle the case. The European Commission announced proposals to strengthen supervision over banks and other financial institutions to toughen up its fight against money laundering and terrorist financing after admitting that present measures have "failed all too often."

The EC wants to give the European Banking Authority, the bloc's supervisory body for financial services, a powerful new mandate to monitor what firms are doing to tackle money laundering.

—Neil Hodge

Poor AML practices illustrated at Danske Bank

Jaclyn Jaeger examines a pending investigation from Denmark's financial crime regulator into Danske Bank for possible money laundering violations related to its Estonian branch.

Compliance and legal troubles at Danske Bank continue to escalate.

On Aug. 6, 2018, Denmark's State Prosecutor for Serious Economic and International Crime (SØIK) announced it had initiated a criminal investigation against Danske Bank for possible money laundering violations related to suspicious transactions connected to the bank's Estonian branch.

"Due to the very serious nature and scope of the case, we have followed the case for a long time," State Prosecutor Morten Niels Jakobsen of SØIK said in a statement. The investigation has now progressed enough where SØIK can finally confirm that it has launched an investigation and is currently determining whether to bring criminal proceedings against Danske Bank for violations of Denmark's Money Laundering Act, he said. Jakobsen added that the case has been a high priority for a long time.

Since Danish prosecutors launched their investigation, "more police reports have been received against Danske Bank in the case," Jakobsen said. Danish prosecutors have obtained a "very extensive" amount of information and material, including from Finanstilsynet (the Danish Financial Supervisory Authority) and are in discussions with several international collaborators, he said.

It's too early to say whether criminal proceedings will result, but no stone will be left unturned, Jakobsen said. Under the Money Laundering Act and the underlying EU Directive, sanctions for money-laundering violations must be effective, proportionate, and dissuasive. "In practice, the determination of fines is based on the size of the total suspicious transactions that a financial institution has not handled correctly," Jakobsen said. "This means that the fine significantly exceeds the profit."

The Danish investigation began in the same week that Estonia's public prosecutor launched an investigation of its own into the bank's money laundering activities. The investigations relate to the now-defunct, non-resident portfolio at the bank's Estonian branch from 2007 to 2015.

The bank has been aware of AML issues for years. In December 2013, senior employees at the bank received a whistleblower report about AML issues in relation to a customer in the Estonian branch's non-resident portfolio (that is, Russian and other non-Baltic customers).

It was not until September 2017, however, that Danske Bank launched an investigation into the non-resident portfolio of the Estonian branch. The investigation covers nine years of data, including more than nine million e-mails, 7,000 documents, and millions of transactions.

Compliance shortcomings

Danske Bank said it received eight orders and eight reprimands from the Danish Financial Supervisory Authority (Danish FSA) on May 3, 2018, regarding management and governance in relation to the AML case at the Estonian branch. "Danske Bank has taken several steps and initiatives to comply with the orders and will continue the work going forward," Danske Bank CEO Thomas Borgen said on a July 18 conference call with investors.

These orders and reprimands follow the findings of a scathing report by the Danish FSA, describing multiple failures by the bank's management team to prevent the money laundering. In its report, the Danish FSA said it "finds it particularly worthy of criticism" that:

- Deficiencies in all three lines of defense at the Estonian branch were so significant that customers had the opportunity to use the branch for criminal activities involving vast amounts;
- The bank did not initiate an investigation into the extent of suspicious transactions and customer relationships until September 2017—more than four years after the termination by one of the branch's correspondent banks of its correspondent bank relations and almost four years after the whistleblower report;
- The bank deferred the decision to close the part of the non-resident portfolio that related to customers who did not have personal or business-related links to the Baltic countries until January 2015 and that the closedown was not completed until January 2016;
- The bank's internal reporting, decision-making processes and corporate culture failed to ensure that the problems of the non-resident portfolio were sufficiently identified and handled in a satisfactory way, including by reporting suspicion of criminal activities to relevant authorities;
- The bank did not inform the Danish FSA of the identified AML issues, even though in early 2014, it should have been clear to some executive board members and other senior employees that the information previously provided by the bank to the Danish FSA and the Estonian FSA in 2012 and 2013 was misleading and that it should have been clear to them that the supervisory authorities focused on the area; and
- The bank's information to the Danish FSA since the beginning of 2017 has been inadequate.

"Consequently, the case has uncovered serious weaknesses in the bank's governance in a number of areas," the report stated. "On this basis, the Danish FSA finds that the bank is exposed to significantly higher compliance and reputational risks than previously assessed."

The Danish FSA acknowledged, however, that the bank has made improvements in its AML and compliance areas in recent years. For example, the bank has stated that it has increased the number of employees working with AML in the first and second lines of defense from less than 200 to 550 in 2017 and nearly 900 today. Among other things, the bank has also expanded and updated internal AML training, worked to strengthen the compliance culture, and made considerable IT investments.

Additionally, the bank in July appointed Philippe Vollot as chief compliance officer and as a new member of the executive board. Vollot will take up his position by Dec. 1, 2018. "With Philippe Vollot as new member of our executive board, we strengthen our competencies within compliance and anti-financial crime, which has been a focus area at Danske Bank in recent years," Borgen said.

Regulatory action

Separately, the Legal Affairs Committee of the Riigikogu (Parliament of Estonia) on July 31 convened a meeting to find out why nobody took responsibility for the money laundering case concerning Danske Bank. "We would like to get answers from the supervisory agency and the investigative bodies on how this criminal deception could be carried out through Estonia for such a long time, and if the authorities have done everything they can to investigate it," Committee Chairman Jaanus Karilaid said in a press statement.

Parliamentary parties have until Sept. 12 to submit opinions on "whether to establish a Riigikogu committee of investigation to deal with the money laundering case, or to form a working group at the Legal Affairs Committee that would investigate this problem in depth," Karilaid said.

She added that the Committee is also considering "whether to change the legal order so that in the future the owner of the money or the conductor of the transaction has to prove the legality of the money." At present, it is up to the state to prove the illegal origin of the money.

In response to the Estonian AML investigation, Borgen acknowledged that the bank had insufficient controls in place. "While it is too early to conclude as to the extent of suspicious transactions, it is clear that

Danske Bank has failed to live up to our own standards and expectations of our stakeholders in terms of preventing our Estonian branch from being used for potential illegitimate activities," he said.

Moving forward, Borgen said, Danske Bank is "committed to transparency with respect to the findings of the investigations, including a clear account of the issues, causes, and accountabilities."

Additionally, the Danske's board of directors and executive board have determined that Danske Bank should forego any profits from the suspicious transactions in the Estonian non-resident portfolio. Any gross income generated from such transactions from 2007 to 2015 will go toward combating international financial crime and other efforts, Danske Bank said.

Findings from the investigations will be reported by September 2018. The final amount to be made available will be decided after the investigations conclude. As it stands now, "we have no insight into any potential fine," Borgen said. "When we have some more clarity, we will communicate that to the market." ■

AML failures

Below is an excerpt from the findings of the report by the Danish Financial Supervisory Authority regarding failures by Danske Bank's management and senior employees to prevent money laundering.

From the end of 2012 to November 2013, Danske Bank did not have a person responsible for AML activities as required by the Danish Anti-Money Laundering Act. The Danish FSA was not notified of this until February 2018, and then as a result of the Danish FSA's supplementary questions. The board of directors and the executive board have stated that in practice, the head of group compliance and AML, who reported to the bank's CFO, was the person responsible for AML activities.

The bank had, and has, organized its management using three so-called lines of defense. The first line of defense is the business itself, which must ensure correct, legal, and expedient operations. The second line of defense is a risk management function that is to identify and mitigate risks and a compliance function that is to check compliance with rules. Finally, the third line of defense is the internal audit department, which monitors whether the first and second lines of defense identify the problems. Management receives reporting from the three lines of defense on an ongoing basis.

The board of directors and the executive board have stated that when assessing the board of directors' and the executive board's work and the volume of written material that the members of the two boards receive, it should be taken into consideration that the branch in Estonia accounts for only a small part of the total business and total risks. They have argued that because of this, management must to a large degree rely on the defense systems in place to function.

When information about the business and the effectiveness of defense systems of a worrying nature comes to light, management attention must, however, increase. At the end of 2013, the branch's assets made up about 0.5% of the group's total assets, while profit before impairments made up about 2.0% of group profit before impairments for the year 2013. In respect of the Estonian branch, there were deficiencies in all three lines of defense.

Source: Danish Financial Supervisory Authority