GIR INSIGHT

EUROPE, MIDDLE EAST AND AFRICA INVESTIGATIONS REVIEW 2020

EUROPE, MIDDLE EAST AND AFRICA

INVESTIGATIONS REVIEW 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-269-5

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

Contents

Preface

Welcome to the *Europe, Middle East and Africa Investigations Review 2020*, a *Global Investigations Review* special report.

Global Investigations Review is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing, telling them all they need to know about everything that matters.

Throughout the year, the *GIR* editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products. In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than our journalistic output is able.

The *Europe, Middle East and Africa Investigations Review 2020*, which you are reading, is part of that series. It contains insight and thought leadership, from 32 pre-eminent practitioners from these regions.

Across 11 chapters, spanning around 150 pages, it provides an invaluable retrospective and primer. All contributors are vetted for their standing and knowledge before being invited to take part. Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other chapters provide valuable background so you can get up to speed quickly on the essentials of a particular topic.

This edition covers France, Germany, Italy, Nigeria, Romania, Russia, Switzerland and the UK from multiple angles; has overviews on trends in anti-money laundering, and how to remediate, to use the parlance, issues inside African business.

Among the gems, it contains:

- a timeline of warnings missed by Danske Bank and other case studies from the fight against money laundering;
- one our best-ever pieces on investigating in Africa – and in particular the extra hurdles faced by anyone seeking to remediate how it operates in the continent;

- all the latest developments from France – where the blocking statute is again on the agenda and a new enforcer has tentatively bared its teeth;
- handy roadmaps for setting up investigations in Germany and Switzerland; and
- how Russia wants to go straight, and the SFO and the FCA's respective years – how successful were they? The verdict appears mixed.

And much, much more. We hope you enjoy the volume. If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you.

Please write to insight@globalinvestigationsreview.com.

Global Investigations Review
London
May 2020

Anti-Money Laundering Trends and Challenges

Deborah Luskin, Anant Modi, Selma Della Santina and Sarah Wrigley
Forensic Risk Alliance

In summary

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations have been increasing. US regulators have historically been the toughest enforcers of AML rules, but their European counterparts have been closing the gap. This chapter describes some of the challenges these organisations may face in ensuring an effective and sustainable AML programme. We focus on the changing legislative environment, emerging trends relating to trade-based money laundering and virtual currencies, and evolving methods making use of machine learning and data sharing; and discuss some of the lessons learned from recent AML scandals and key elements that should be present in a robust AML programme.

Discussion points

- In 2019, European authorities exceeded US-ordered AML penalties
- 95 per cent of system-generated alerts are closed as 'false positives' in the first phase of review, costing billions of dollars in wasted investigation time
- As of March 2020, the requirement to publish publicly accessible ultimate beneficial owner lists had not been implemented by 17 EU member states
- Regulators have been encouraging the use of innovative approaches, such as AI and machine learning to more effectively identify suspicious activity.
- Lessons learned from recent scandals

Referenced in this article

- Danske Bank
- European Commission
- Financial Action Task Force
- Financial Crimes Enforcement Network
- US Federal Financial Institutions Examination Council

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations have been increasing. Globally, there were 58 AML penalties in 2019 totalling US$8.14 billion as compared to 2018 when there were 29 penalties totalling US$4.27 billion.[1] US regulators have, historically, been the toughest enforcers of AML rules, but their European counterparts have been closing the gap. Between 2014 and 2017, AML fines from European supervisors totalled US$214 million while those from US regulators totalled US$1.96 billion. In 2019, European authorities actually exceeded US-ordered AML penalties, totalling US$5.8 billion against US$2.2 billion.

To provide context as financial institutions and companies plan their response to this rapid pace of strengthening enforcement in Europe, this chapter describes some of the challenges these organisations may face in ensuring an effective and sustainable AML programme. We focus on the changing legislative environment, highlighting trends and methods on the authorities' radar. This includes emerging trends relating to trade-based money laundering and virtual currencies, and evolving methods making use of machine learning and data sharing. Finally, we discuss some of the lessons learned from recent AML scandals and key elements that should be present in a robust AML programme.

AML challenges

Identifying ultimate beneficial owners

A critical component in combatting money laundering is understanding who your customer is, who the ultimate beneficial owners (UBOs) are and the nature of their business. Regulators expect financial institutions to determine who the beneficial owners are. That said, determining the UBO is notoriously difficult, especially when customers provide false information or use corporate vehicles in secrecy havens. Even when these lists are made available, such as with the UK's Companies House, the information provided is not consistently verified.[2, 3] When compliance personnel attempt to verify customer-provided UBO information, it can be a timely and costly process. Where banks have correspondent banking relationships, there are additional costs involved in understanding the UBO for the respondent bank's customers. Until 2020, most countries did not publish ownership structures on public domains so the information provided to financial institutions was more difficult to verify. Later in this chapter, we discuss the existing and pending legislation that aims to make such lists mandatory and transparent, and discuss some examples of entities who have been attempting to share information regarding UBO in a more efficient and cost effective manner.

1 '$8.14 billion of AML fines handed out in 2019, with USA and UK leading the charge.' *Encompass* (https://www.encompasscorporation.com/blog/encompass-aml-penalty-analysis-2019/).

2 'How Britain can help you get away with stealing millions: a five-step guide.' *The Guardian* (https://www.theguardian.com/world/2019/jul/05/how-britain-can-help-you-get-away-with-stealing-millions-a-five-step-guide).

3 'Companies House regime faces major overhaul.' *Accountancy Daily* (https://www.accountancydaily.co/companies-house-regime-faces-major-overhaul).

Leveraging technology

There is a regulatory expectation that institutions monitor customer activity to identify suspicious patterns or behaviour. This can only be achieved successfully when an institution effectively aggregates their data across systems, divisions and geographic locations. However, transactional data is often held in different repositories (eg, card services, deposit operations) and in numerous legacy systems due to previous acquisitions, thus making it difficult to connect common characteristics and limiting the effectiveness of transactional monitoring and analysis. If the disparate data could be analysed as a group, it would likely improve the ability to identify potentially unusual or dubious transactional activity such as those that do not appear to align with the customer's expected business operations. For example, Credit Suisse and UBS have developed solutions that utilise a data lake for the purpose of aggregating disparate data for analysis.[4, 5] In UBS's case, they joined up old databases with fast moving trading data, thereby combining two data types for the first time to provide actionable insight.[6]

Another reason to work towards aggregating data from multiple sources is that criminal organisations often launder their funds between multiple financial institutions. It is often more difficult to identify a problematic transaction with information from only one hop in a series of money transfers. Fortunately, there are opportunities to voluntarily exchange information to more accurately identify fraud and money laundering. In some jurisdictions, there are laws or task forces that provide for such data exchange, including section 314(b) of the US PATRIOT Act and the UK National Crime Agency Joint Money Laundering Intelligence Taskforce (JMLIT). We discuss some examples of these public–private information-sharing partnerships later in this chapter.

The cost of false positives

Financial institutions typically have transaction monitoring systems that apply rules-based conditions to identify suspicious transaction behaviour, such as excessive cash deposits, rapid money movement from one bank to another and structured transactions. Transactions that violate these rules generate an alert, which is then reviewed. Despite decades and billions of dollars in industry investment, over 95 per cent of system-generated alerts are closed as 'false positives' in the first phase of review, with approximately 98 per cent of alerts never resulting in a suspicious transaction report (STR).[7] Reviewing false positive alerts costs billions of dollars in

4 'Credit Suisse offers a brand new and effective reporting service.' *Waters Technology* (https://www.waterstechnology.com/waters/analysis/2480247/aftas-2016-best-reporting-initiative-credit-suisse).

5 'UBS's Data Lake for Regulation Pays Dividends.' *Waters Technology* (https://www.waterstechnology.com/data-management/4412476/ubss-data-lake-for-regulation-pays-dividends).

6 'Companies all over the world use Dremio's data lake engine to power their data lakes.' *Dremio* (https://www.dremio.com/customers/).

7 'Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states.' *Reuters*, 14 March 2018 (https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV).

wasted investigation time each year. The greater the number of false positives, the more expensive it is to onboard customers and process payments. They also expose financial institutions to fines and reputational damage.

AML detection is often automated, but generally not predictive. For example, automated tools may be configured to identify suspicious transactions based on typical red flags, such as rapid, successive transfers of money. However, if a machine learning solution was used to analyse the totality of customer and transactional data, entities could begin to identify unusual patterns worth investigating before they become known red flags. Regulators are increasingly encouraging such uses of artificial intelligence and machine learning solutions, as we discuss later in this chapter.

Regulatory changes

The primary legislation in the US governing AML has grown over time from the Bank Secrecy Act (BSA) of 1970, to the Money Laundering Control Act of 1986 and sections within the US PATRIOT Act of 2001. The guidance continues to change, for example, with the inclusion of virtual currency providers in 2013 and the Customer Due Diligence (CDD) Rule requiring verification of customers in 2016. The US has been criticised in its last two Financial Action Task Force (FATF) Mutual Evaluation Reports (MERs) for the lack of transparency when it comes to identifying UBOs. As of October 2019, legislation was passed in the US House of Representatives, the Corporate Transparency Act, which would require legal entities to disclose their beneficial owners. If the companion legislation, the ILLICIT CASH Act, is passed in the US Senate, it would grant the Financial Crimes Enforcement Network (FinCEN) the authority and responsibility to collect and maintain corporate ownership data.

There has been even more rapid change and advancement occurring in EU legislation, but with varying levels of implementation. A series of Anti-Money Laundering Directives (AMLDs) were passed between 1991 and 2019, the most recent including the fifth AMLD (5AMLD, effective 10 January 2020) and the sixth AMLD (6AMLD, effective 3 December 2020). Some of the more prominent additions within the 5AMLD included extending AML rules to additional providers such as virtual currency exchange service providers and dealers in high value goods. It also reduced anonymous prepaid card limits to €150, banned cards issued outside the EU unless they have comparable AML regimes, made UBO lists public within 18 months, mandated functional public politically exposed persons (PEP) lists and enhanced due diligence (EDD) measures to monitor transactions with high-risk countries. The 6AMLD focuses on aligning 22 predicate crimes, includes 'aiding and abetting' to the definition of money laundering, extends criminal liability to legal persons and increases the maximum imprisonment from one to four years. Each directive must be transposed into law within each member state and the enforcement of those laws is handled separately in each jurisdiction. As of March 2020, the requirement to publish publicly accessible UBO lists has not been implemented by 17 of the EU member states and many of the member states have restricted access to their UBO data.[8]

8 'Patchy Progress in Setting up Beneficial Ownership Registers in the EU.' Global Witness. Published 20 March 2020.

Recent typology trends

As with most types of crime, when one money laundering method becomes more challenging to execute, perpetrators will seek out new methods. As legislation has become more stringent and financial institutions have correspondingly strengthened their processes, criminals' preferred methods have shifted as well. While there are numerous money laundering typologies, this section focuses on two that are receiving more attention from regulators and appear to be increasing in prominence.

Trade-based money laundering

As more governments around the world impose AML obligations on the banking sector, money laundering activity has increasingly shifted towards the non-bank financial sector, non-financial businesses and professions. FATF defines trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise illicit origins. [9] TBML is increasingly viewed as the weakest link in combating money laundering.[10] US law enforcement agencies have also noted an increase in TBML, which they attribute, in part, to more stringent anti-money laundering laws and improved compliance efforts by financial institutions.[11]

The three broad methods of TBML noted by FATF are:

- using financial institutions;
- physically smuggling cash between countries; and
- using the international trade system.

A 2006 FATF report said that of the three methods, the abuse of the international trade system had received relatively little attention.[12]

TBML is notoriously difficult to detect because it is integrated into the economy through a trade transaction. Red flags that may indicate potential TBML include material discrepancies between the invoices and the fair market value of goods, payments to a vendor by unrelated third parties, discrepancies between the shipment and import or export stated business purpose, trade transactions that do not match the businesses involved, duplicate invoicing and unusual shipping routes or transshipment points. The counterparties in transactions typically have access to most, if not all, of these documents. For financial institutions, they would typically only have access to some of these detailed documents where they have issued letters of credit. For open account trading, financial institutions must primarily rely on the information contained in the SWIFT payment messages.

9 'Trade Based Money Laundering.' Page 1. FATF. Published June 2006.

10 'Uncontained.' *The Economist*. Published May 2014.

11 'Countering Illicit Finance and Trade: U.S. Efforts to Combat Trade-Based Money Laundering,' US Government Accountability Office. Published December 2019.

12 'Trade Based Money Laundering.' Page 5. FATF. Published June 2006.

To counter the risk of enabling TBML, companies should assess their risk and consider such red flags. Financial institutions should factor TBML in their risk assessment and implement sufficient controls for reviewing trade documentation supporting letters of credit and how they monitor the payment messages for open trade transactions. For financial institutions who offer trade credit, The Wolfsberg Group has issued revised trade finance guidance in 2019.[13]

Virtual currencies

Virtual currencies are increasingly used as a vehicle for money launderers, drawn to the increased anonymity they provide. Virtual currencies exist as data entries on a publicly distributed online ledger called a blockchain. The entries represent records of transactions in blocks, similar to a traditional ledger. The entries are secured using cryptography, which protects the transactions executed from modification or double spending. Global money laundering syndicates have begun moving illicit proceeds into and through virtual currencies as another method of layering transactions in order to hide the origin of dirty money.[14]

The US Department of Homeland Security forecasts that illicit use of virtual currency will accelerate due to its unique features and ongoing efforts to further improve anonymity. Law enforcement investigations have shown that many virtual currency users who buy or sell illegal goods or exchange virtual currency on darknet markets rely on technology that conceals their location and identity from law enforcement. Anonymising software such as the Tor network can obscure the source and destination of virtual currency and make it more difficult for law enforcement to link transactions to people, virtual currency wallets or IP addresses. FinCEN notes that anonymity-enhanced cryptocurrencies (AECs) specifically designed to make virtual currency transactions untraceable and to provide near-impenetrable anonymity are increasingly being used on the darknet.[15]

However, despite its growing use, constraints in scale, liquidity and market value volatility suggest that virtual currency has not yet surpassed the use of physical currency or the traditional financial system for large-scale money laundering. Although the darknet and virtual currencies allow for illicit cross-border transactions, eventually criminals exchange their virtual currency for paper currency, requiring the use of a virtual currency exchanger. In the US, based on facts and circumstances, virtual currency exchangers and administrators are subject to the BSA and FinCEN actively penalises entities that fail to comply.[16]

On a global basis, regulators are strengthening legislation and publishing guidance for addressing the risks of convertible virtual currencies (CVCs). FinCEN issued an advisory regarding virtual currencies in May 2019, which listed 30 red flags that may indicate the abuse of

13 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles, 2019 amendment.' The Wolfsberg Group. Published 27 March 2019.

14 'National Money Laundering Risk Assessment.' Page 3. U.S. Department of Treasury. Published 2018.

15 'Advisory on Illicit Activity Involving Convertible Virtual Currency.' FinCEN. Published 09 May 2019.

16 In March 2013, FinCEN formally stated that a 'money transmitter', as defined in the BSA, included virtual currency exchanges and administrators of centralized repositories of virtual currency who have the authority to both issue and redeem the virtual currency.

Case studies: FinCEN

BTC-e: FinCen's first penalty against a foreign-located money service business

Within the US, entities that facilitate the transmission of CVCs, such as Bitcoin, Monero and Ether, are required to register with FinCEN as a money service business (MSB) and are subject to the BSA requirements. This also includes peer-to-peer (P2P) exchangers, which exchange fiat currencies for virtual currencies or one virtual currency for another.

In July 2017, FinCEN issued its first penalty against a foreign-located MSB. The company, BTC-e, was an internet-based money transmitter that exchanged fiat currency as well as the CVCs Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. FinCEN found that BTC-e facilitated transactions involving numerous criminal activities. They were cited for lack of customer due diligence, the knowing transmission of currency for criminal activities and performing services for entities flagged under section 311 of the USA PATRIOT Act as primary money laundering concerns. They were fined US$110 million.[i]

FinCEN's first enforcement action against Peer-to-peer virtual currency exchanger

In April 2019, FinCEN assessed its first civil penalty against an individual who operated as a P2P exchanger of CVC. In this case, the individual conducted over 200 transactions involving the physical transfer of more than US$10,000 in currency. Each of those transactions alone required the filing of a currency transaction report (CTR). FinCEN cited the individual for failing to register as an MSB, for the lack of AML policies and procedures as required by the BSA, and for not reporting suspicious transactions. In addition to his fine, the individual is permanently banned from ever performing money transmission services again.[ii]

i 'FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net. Drug Sales.' FinCEN (https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware).

ii 'FinCEN penalizes peer-to-peer virtual currency exchanger for violations of anti-money laundering laws.' FinCEN (https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money).

virtual currencies.[17] FATF modified Recommendation 15 to explicitly include financial activities involving virtual assets. When the 5AMLD became effective in January 2020, EU member states included virtual currency providers within the set of obliged entities that are subject to AML regulations; specifically, they are now required to perform customer due diligence

17 'Advisory on Illicit Activity Involving Convertible Virtual Currency.' FinCEN. Published 09 May 2019.

and submit suspicious activity reports (SARs). In addition, the 5AMLD introduced rules that require providers of cryptocurrency exchanges and wallets to be registered with the competent authorities in their domestic locations; for example, the UK's Financial Conduct Authority.

Evolving methods for combating money laundering

Using artificial intelligence and machine learning to detect money laundering

Regulators have been encouraging the use of innovative approaches, such as AI and machine learning to more effectively identify suspicious activity. A joint statement issued by various US regulators in December 2018 described two methods in particular: [18]

- building or enhancing innovative internal financial intelligence units devoted to identifying complex and strategic illicit finance vulnerabilities and threats, and
- experimenting with AI and digital identity technologies applicable to their BSA or AML compliance programme.

The joint statement made note of the benefits of such innovative technologies, including strengthening AML compliance programmes, enhancing transaction monitoring capabilities and maximising the use of compliance resources. Interestingly, it was also stated that banks would not be penalised for failures in a pilot programme of this nature and where new technology identified transactions that were not captured under existing rules-based systems, those would not necessarily result in supervisory action. Similarly, the Singapore Police Force and Monetary Authority of Singapore published a paper in 2018 to encourage greater adoption of data analytics and provided an example of one bank that used machine learning to reduce false positives and increase true positives.[19] Germany's regulator, the Federal Financial Supervisory Authority, produced a comprehensive report that same year to evaluate the benefits and risks in using artificial intelligence:

> *Big Data Artificial Intelligence makes it easier to identify anomalies and patterns. It increases the efficiency and effectiveness of compliance processes, such as the prevention of money laundering and fraud.*[20]

There are financial institutions that have performed pilot programmes utilising machine learning solutions within their AML compliance programmes. United Overseas Bank underwent a six-month pilot trial for an AML machine learning solution used for name screening and

18 'Joint Statement on Innovative Efforts to Combat Money Laundering.' FinCEN. Published 3 December 2018; issued by the U.S. Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), Financial Crimes Enforcement Network (FinCEN), National Credit Union Administration (NCUA), and Office of the Comptroller of the Currency (OCC).

19 'Financial industry shares good data analytics use cases to fight financial crime.' Monetary Authority of Singapore (https://www.mas.gov.sg/news/media-releases/2018/financial-industry-shares-good-data-analytics-use-cases-to-fight-financial-crime).

20 'Study: Big Data meets artificial intelligence.' BaFin (https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html).

transaction monitoring. For name screening, they reported a 50–60 per cent reduction in false positives. For transaction monitoring, they reported a five per cent increase in true positives and 40 per cent drop in false positives. When their system spots a pattern of suspicious activity, it creates a smart rule and adds it to their AML typology library so they can potentially detect future instances of that pattern.[21] Nokia, OP Group, SEB and Standard Chartered have all partnered with a machine learning solution provider for trade finance-related document checks, in which the software checks the documents for AML and compliance issues.[22]

Sharing information to combat money laundering

Money launderers often move funds between jurisdictions to make it more difficult to investigate and trace the source of funds. There has been guidance encouraging the sharing of information related to money laundering for quite some time to address this issue. The FATF has made several recommendations regarding the sharing of information, as do some national regulators. However, these efforts focused primarily on information sharing between law enforcement and Financial Intelligence Units (FIUs) across jurisdictions. While those efforts are critical in identifying and combatting money laundering, we now see a trend of public–private partnerships and, in some cases, financial institutions sharing information directly with each other.

Stricter regulations for correspondent banking relationships have caused many financial institutions to 'de-risk' by closing those relationships. According to the Bank for International Settlements (BIS), active relationships in the correspondent banking network declined by about 20 per cent between 2011 and 2018, even as the value of payments increased.[23] This has the negative side effect of limiting banking services to areas in need and potentially causing some entities to find less reputable routes of transferring money. Information sharing regarding UBO could address some of the risk inherent in correspondent banking relationships.

A challenge that arises in public–private information sharing is navigating legislation with regard to protection of personal data. For a private company or bank to share client data, a legal mechanism must first be established. There are several examples of public-private partnerships that have done so successfully, as shown in the boxout overleaf.

Lessons learned from recent scandals

Russian money and weak controls

There have been a number of high-profile AML scandals in European banks in recent years, including ABLV Bank, Danske Bank, Swedbank, Deutsche Bank, Pilatus Bank and ING Group. From media reports, what most of these money laundering scandals appear to have in common are weaknesses in their AML controls that allowed vast amounts of money flowing from Russia

21 'UOB adopts machine learning tools to combat financial crime.' *Finextra* (https://www.finextra.com/newsarticle/32573/uob-adopts-machine-learning-tools-to-combat-financial-crime).

22 'Nokia and three banks pilot machine learning solution to automate compliance checks.' *Global Trade Review* (https://www.gtreview.com/news/fintech/nokia-and-three-banks-pilot-machine-learning-solution-to-automate-compliance-checks/).

23 'On the global retreat of correspondent banks.' Bank for International Settlements (https://www.bis.org/publ/qtrpdf/r_qt2003g.htm).

Examples of public–private information sharing in Europe, the Middle East and Africa

Nordic countries

The five largest lenders in the Nordics – Danske Bank, BNB, Handelsbanken, Nordea and SEB – disclosed plans to share Know Your Customer (KYC) data on large and mid-size corporations with the goal of streamlining due diligence, similar to the initiative by the Dutch major banks.

Netherlands

At the encouragement of the Dutch regulator, in 2019, four Dutch banks – ABN Amro, Rabobank and Volksbank – signed a covenant with the National Police and the Financial Intelligence Unit to help identify people who facilitate crime. The authorities believe a small group of 'enablers', financial advisers, tax advisers, notaries, accountants and lawyers play a key role in laundering drug money in the Netherlands. The law enforcement agencies will provide information to the banks who will compare it to their KYC and transaction data.

Separately, the three largest banks in the Netherlands, ABN Amro, ING and Rabobank began a pilot programme to share KYC information, such as data on beneficial owners and organisational charts, where those clients have consented. They are trying to determine whether or not this information-sharing can reduce costs and give compliance departments access to better, more timely KYC data.

United Arab Emirates

In February 2020, licensing authorities and six banks in the UAE announced a plan to use blockchain technology to share verified data about customers.

United Kingdom

The UK's JMLIT is a partnership between law enforcement and financial institutions where they exchange information related to financial crime, including money laundering. Since its inception in 2015, JMLIT has supported numerous law enforcement investigations while the participating financial institutions have identified over 5,000 accounts suspected of money laundering, begun 3,500 of their own internal investigations and used the information obtained to enhance their systems of controls and monitoring. In addition to suspicious accounts, they can also share information related to emerging typologies that may allow financial institutions to identify suspicious behaviour at an earlier stage.

and the former Soviet states into the EU and US financial system.[24, 25] As examples, in 2005, Swedbank acquired Hansabank and shortly thereafter rebranded its Baltic state branches in Estonia, Latvia and Lithuania. In 2006, Danske Bank acquired Sampo Bank and reorganised the Baltic state subsidiaries as branches. These smaller Baltic market branches were criticised by regulators for weak controls, effectively serving as intermediaries between money in the former Soviet states and the large financial centres of Europe and the United States.[26, 27]

In July 2019, the European Commission (EC) published an analysis of the recent money laundering failures involving EU financial institutions. They identified four common themes in their AML failures, all of which emanate from leadership.[28]

- Ineffective or lack of compliance with the legal requirements for anti-money laundering. In many cases, financial institutions did not 'prioritise' compliance with AML legislation in their policies. In other cases, there was no evidence that any risk assessment was performed.
- Governance failures in relation to AML. Deficiencies in AML governance structures included one or more of the 'three lines of defence,' internal reporting, group policies and senior management's responsibilities and accountability.
- Misalignments between risk appetite and risk management. Certain institutions may have actively pursued business in high-risk jurisdictions and based their business model almost entirely of non-resident deposits without implementing corresponding controls. More specifically, they found that several financial institutions were willing to accept PEPs or companies where a beneficial owner could not be identified.
- Negligence of group AML policies. In some instances, there were insufficient group-wide AML policies. Further, they found that the parent did not appear to have a sufficient understanding of the risks throughout their financial institution.

While deficiencies in basic AML controls are always concerning, the report points out that these institutions were engaging in high-risk business and thus should have had even greater impetus to implement a robust and effective AML programme. The board of directors and

24 'Europol highlights Russian money as biggest laundering threat.' *Reuters* (https://www.reuters.com/article/us-europe-moneylaundering-europol/europol-highlights-russian-money-as-biggest-laundering-threat-idUSKCN1TE2K6).

25 'The Fallout from Russian Money Laundering Continues to Grow for European Banks.' *International Banker* (https://internationalbanker.com/banking/the-fallout-from-russian-money-laundering-continues-to-grow-for-european-banks/).

26 'Danske reprimanded over weak money-laundering controls.' *Financial Times* (https://www.ft.com/content/387daede-4eac-11e8-a7a9-37318e776bab).

27 'Estonia warns of risks in wake of money laundering scandal.' *Reuters* (https://www.reuters.com/article/us-moneylaundering-estonia/estonia-warns-of-risks-in-wake-of-money-laundering-scandal-idUSKCN1TP1VS).

28 'Report From the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions.' European Commission. Published 24 July 2019.

executive management are responsible for creating a culture of compliance, performing a robust and tailored risk assessment, and ensuring the implementation of an AML programme that addresses risks identified in the risk assessment, including specific, verifiable controls.

Understand legacy risk and be proactive

To assess an entity's risk requires an understanding of the historical transactions – 'legacy risks'.[29] In many of the recent AML scandals, suspicious accounts were already closed at the time the potential money laundering became widely known; however, the underlying transactions that indicated possible predicate crimes had been approved and processed, and in many instances, not reported to the respective financial intelligence unit in accordance with AML regulations.

The timeline of events at Danske Bank, as reported in the media, indicates that there had been warning signs. This issue is certainly not restricted to Danske Bank. There are other examples of financial institutions who have closed down higher-risk business lines where it appears that the extent of potential money laundering related issues were not taken into account and where further action may be required. Even after accounts are closed, however, there may be obligations to report suspicious activities and potential sanctions violations. Former account owners or controllers of those closed accounts may hold or control other accounts at the institution (or 'obliged entity'), which remain active if the relationship and purpose of those accounts are not identified or determined. These unknown areas present a lingering risk that should be fully examined and understood, addressed internally and potentially reported to the appropriate authorities.

Inconsistent laws and supervision

The EU would benefit from a centralised AML supervisor as it would allow them to not only address the pervasive cross-border elements to money laundering, but apply the same standards across the EU so money launderers do not look for weak spots to exploit. In a European Parliament (EP) analysis paper, it was acknowledged that a series of AML rule breaches in European banks has raised doubts about the effectiveness of EU bank supervision. They point out that research performed by the International Monetary Fund against FATF's MERs shows there is a positive correlation between the size of a country's GDP and the strength of and compliance with their AML standards.[30]

While the EU has strengthened its AML legislation, supervision and enforcement by EU member states has been reportedly applied inconsistently. EU member states are required to transpose the AMLDs into national law by a prescribed date. In February 2020, the EC sent

29 Ahlberg, Michaela, and Anna Romberg. *The Grey Zone: A Practical Guide to Corporate Conduct, Compliance and Business Ethics*. Vulkan, 2019.

30 'The Supervisory approach to anti-money laundering: an analysis of the Joint Working Group's reflection paper.' Page 13. European Parliament. Published November 2018.

Case study: Danske Bank

Between 2007 and 2015, there were approximately 10,000 customers reportedly in the non-resident portfolio at Danske Bank. During that timeframe, payments totalling €200 billion flowedd through the Estonian branch.

Timeline

- 2013: A whistleblower at the Estonia branch emailed a report titled, 'Whistleblower disclosure – knowingly dealing with criminals in Estonia branch'.
- February 2014: The bank conducted an on-site audit in Estonia and in draft conclusions sent by email, said: 'we cannot identify actual source of funds or beneficial owners'. A branch employee 'confirmed verbally that the reason underlying beneficial owners are not identified is that it could cause problems for clients if Russian authorities request information'.
- End-2015: The international banking division at Danske Bank was closed and the non-resident portfolio terminated.
- Early 2016: Denmark's financial regulator reported Danske Bank to the police for breaching AML rules.
- December 2017: Danske was fined US$1.9 million by a public prosecutor for violating AML rules.
- July–August 2018: Estonian and Danish prosecutors launched criminal investigations.
- October 2018: US Department of Justice launched a criminal investigation into the Estonian branch.

legal warnings to eight EU countries who have not yet fully incorporated the 5AMLD elements into national law.[31] In some recent AML scandals, country supervisors only took action after FinCEN took special measures[32] or investigative journalists uncovered wrongdoing.[33]

Partly in response to these circumstances, in November 2019, the finance ministers of France, Germany, Italy, Latvia, the Netherlands and Spain issued a joint position paper. If the proposal is adopted, it would create a centralised AML supervisor with EU-wide authority in Europe. Not all country representatives are supportive of such a plan. Kaja Tael, permanent representative to the EU from Estonia, stated, 'National authorities have a lot to offer – they have the local know-how, the ability to react quickly, but the international cooperation needs to

31 'European Commission warns eight countries over late AML laws.' Fintech Futures (https://www.fintechfutures.com/2020/02/european-commission-warns-eight-countries-over-late-aml-laws/) Note: The eight countries were Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain.

32 'Why the U.S. Treasury Killed a Latvian Bank,' *Forbes* (https://www.forbes.com/sites/francescoppola/2018/02/28/why-the-u-s-treasury-killed-a-latvian-bank/#51901b497adc).

33 'Swedish TV says Swedbank linked to Baltic money laundering scandal,' *Reuters* (https://www.reuters.com/article/danske-bank-moneylaundering-swedbank/swedish-tv-says-swedbank-linked-to-baltic-money-laundering-scandal-idUSL5N20F1EH).

be improved.' Jörg Kukies, state secretary at Germany's Federal Ministry of Finance, expressed support for a new anti-money-laundering supervisor, as well as surprise over the optimism expressed by other country representatives regarding the strength of national-level supervision. He stated, 'We have seen so many cases of very obvious deficiencies in our rule sets. I think we have to be very self-critical about the degree of weakness in individual member states.'[34]

The European Banking Authority (EBA) published a report that evaluated the effectiveness of member state supervisory approaches to AML compliance within banks. They identified some areas of weakness across the supervisors reviewed. These include the need to assess the effectiveness of controls versus confirming a prescriptive set of requirements, taking proportionately and sufficiently dissuasive corrective measures where AML measures are ineffective and working effectively with domestic and international stakeholders.[35] These criticisms, particularly the rigor of supervisory audits and severity of penalty where weaknesses are found, mirror the criticisms that were widely discussed in the wake of the recent European AML scandals.

Key elements in an AML programme

A study from 2005 showed that, in addition to the penalty a financial institution incurs for an AML failure, they also lose share value and business opportunities due to the reputational damage. Furthermore, remediation costs over the first 18 months are typically 12 times greater than the fine itself.[36] Proactively addressing weaknesses in an AML compliance programme is a smart long-term proposition. The US Federal Financial Institutions Examination Council (FFIEC) publishes a comprehensive inspection manual, which outlines the key elements of a BSA or AML programme.[37] Table 1 identifies key elements from the FFIEC manual and our suggested questions to guide your organisation's planning.

Conclusion

AML risk management has become more challenging over time as the regulations have become more stringent and financial institutions, in particular, have faced larger fines where compliance programs have been deficient. However, it is also a time when more detailed guidance is developed by governmental[38] and non-governmental[39] bodies to help build a robust AML

34 'EU Takes First Steps to Establish Anti-Money-Laundering Supervisor', *The Wall Street Journal* (https://www.wsj.com/articles/eu-takes-first-steps-to-establish-anti-money-laundering-supervisor-11575574443).

35 'EBA Report on Competent Authorities' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks.' European Banking Authority. Published 05 February 2020.

36 'Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states.' *Reuters* (https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV).

37 'BSA/AML Examination Manual.' Federal Financial Institutions Examination Council (FFIEC). Published 2014.

38 'Financial Crime Guide: A firm's guide to countering financial crime risks (FCG).' Financial Conduct Authority. Published February 2020.

39 'Sound management of risks related to money laundering and financing of terrorism.' Basel Committee on Banking Supervision. Published 07 June 2017.

Table 1

US FFIEC's key elements to a BSA or AML programme	Key questions for your organisation to consider
Risk Assessment The risk assessment should identify the specific risk categories applicable to the institution (eg, products, services, customers, geographies) and then contain a more detailed description of the specific risks within those categories that are applicable to the institution.	• Is there a documented risk assessment? • Does the risk assessment include all relevant risks? • Are the risks sufficiently articulated, internal controls rigorously assessed as to their ability to prevent or detect such an event occurring; have actions been identified which directly impact on the occurrence of such risk; and how often and under which circumstances is the risk assessment updated?
AML Compliance Programme The AML compliance programme should be documented and approved by the board of directors.	• Is the AML programme properly documented with sufficiently detailed policies and procedures? • Are controls in place to ensure compliance with policies and procedures outlined in the AML programme? • Do the policies, procedures and controls outlined in the AML programme sufficiently correspond to and mitigate the risks outlined in the risk assessment? • Do the controls outlined identify higher-risk operations, provide reporting methods to the board of directors, identify personnel responsible for AML compliance, address record-keeping requirements, implement risk-based customer due diligence policies, contain detailed procedures for suspicious transaction reporting, address segregation of duties and address the process for anomalous transaction reporting? • Are AML responsibilities included within job descriptions? • Are employees trained in their responsibilities related to AML?
Independent Testing The controls outlined in the AML compliance programme should be subject to independent testing by a suitably experienced person whether from internal audit, external audit, consultants or other qualified parties.	• Is there independent testing of the AML programme (including risk assessment and controls)? • Is the testing performed in a risk-based fashion? • Does the testing include evaluation of the risk assessment, policies and procedures, deficiency remediation, training, suspicious activity monitoring and the relevant information systems used within the AML programme? • How often does independent testing occur? • Are the results of the testing communicated to the board of directors? • Do the results of such testing inform future revisions of the AML risk assessment?
Training All relevant personnel should be trained in both regulatory requirements and the entity's AML policies and procedures. The training should be specific to the organisation. For example, a bank's training may focus on transaction monitoring whereas a shipping company may focus on how to identify red flags in trade-based money laundering.	• Does the training cover all relevant personnel? • Does the training incorporate lessons learned from their industry or institution? • Is the training tailored to the person's specific responsibilities? • Do those charged with overseeing the AML programme receive regular training regarding regulatory requirements? • Is the board of directors and executive management informed of their AML regulatory requirements?

programme, technology is developed to help entities become increasingly sophisticated in their ability to detect and monitor suspicious transactions, and partnerships are developed to share information that allows a more comprehensive compliance effort.

When evaluating your compliance efforts, entities should be proactive, develop a robust AML compliance programme and pay particular attention to the CDD and UBO elements of that programme. As part of this effort, entities should:

- keep up to date on the changing typologies and ensure they are considered in their risk assessment;
- consider opportunities to utilise technology that more intelligently identifies anomalies and suspicious activity;
- where possible, share information when it allows a more comprehensive solution to identifying money laundering; and
- where needed, perform a comprehensive review to understand legacy risk.

Deborah Luskin
Forensic Risk Alliance

Deborah Luskin is an associate director based between Forensic Risk Alliance's Washington, DC office and Europe. She has over 13 years' experience in auditing and consulting, including forensic accounting, financial audit attestation, risk management assessments, Sarbanes-Oxley 404 readiness and audit attestation and service organisation internal control assessments. Deborah's experience at FRA has included forensic accounting support for a financial institution's anti-money laundering review, working with a global manufacturing firm accused of bribery in connection with a Middle Eastern entity, supporting a corporate monitorship of a Tier 1 financial institution and assisting a global manufacturing company and its external counsel in response to an investigation by the Serious Fraud Office and the National Financial Prosecutor's Office into bribery and corruption. Prior to joining FRA, Deborah spent nine years at a Big Four company working in risk management and leading large multinational teams on projects covering various industries.

Deborah is a certified public accountant, a certified anti-money laundering specialist, a certified global sanctions specialist, a certified fraud examiner, is certified in financial forensics, is a certified information systems auditor and a certified information systems security professional. She has a graduate certificate in taxation from American University and a MBA from the University of California, Irvine.

Anant Modi
Forensic Risk Alliance

Anant Modi is a partner in Forensic Risk Alliance's London office in the forensic accounting team. He has over 25 years' experience of providing forensic and accounting services, in particular leading fraud and regulatory investigations, working directly for financial institutions, alongside lawyers or on behalf of regulators. Prior to joining FRA, Anant spent 20 years in the forensic team at a Big Four accounting firm. His experience covers investigations undertaken throughout the United States, Europe, the Middle East and Asia. He has investigated allegations of misconduct (such a rogue trading), market abuse (such as FX market manipulation), financial mis-selling, bribery and corruption, accounting misstatement, embezzlement, procurement fraud, sanctions breaches, among others.

Anant has led a number of assignments within the financial services sector, including anti-money laundering and sanctions compliance, assisting regulators investigate allegations of rogue trading and market abuse, and as part of a monitorship team for US regulators in relation to a deferred prosecution agreement. Most recently, Anant led a money laundering investigation in the Nordics involving Baltic banking subsidiaries and is part of a monitorship team for US regulators in relation to a deferred prosecution agreement with a multinational financial institution.

Anant is a fellow of the Institute of Chartered Accountants in England and Wales.

Selma Della Santina
Forensic Risk Alliance

Selma is a director in the Forensic Risk Alliance Zurich office. She has over 13 years' experience in forensic accounting, financial due diligence and auditing. She specialises in responding to regulatory enforcement requests in the financial services industry. She also has significant experience designing and improving financial crime compliance programmes as well as implementing remediation efforts as a result of past infractions covering various types of fraud risk. Selma has a deep understanding of complex client structures in Swiss private banking as well as of local and international regulatory environments relating to financial crime.

Prior to joining FRA, Selma worked in Big 4 firms in Australia, Austria, Slovenia and Switzerland. She led large international teams to investigate, remediate and assess financial crime infractions, working alongside in-house investigations teams and external legal counsel.

Selma is a certified fraud examiner and holds a MBA, a bachelor of business in finance and accounting, and a bachelor of arts in Italian. She is an Ethic Intelligence certified ISO 19600 and ISO 37001 certified auditor. She is fluent in English, Italian, Bosnian and Slovene.

Sarah Wrigley
Forensic Risk Alliance

Sarah is a director in the Forensic Accounting team based in FRA's London office. She has over 17 years' experience of complex and often cross-jurisdictional investigations, including financial crime, regulatory issues and accounting irregularities. She has worked across a range of industries, focusing particularly on financial services and undertaking investigations across Europe, the Middle East, Africa and Russia.

Before joining FRA, Sarah was the Africa and Middle East Regional Head of Financial Crime Intelligence and Investigations for Standard Chartered Bank, based in Dubai. Sarah led the bank's regional investigation response to global financial crime issues generating media and regulatory scrutiny, such as the 'Panama Papers', the 'Russian Laundromat' and the 1Malaysia Development Berhad allegations. She led a team developing proactive intelligence on emerging financial crime themes covering money laundering and predicate offences, terrorist financing and potential sanctions breaches in order to identify and investigate higher risk clients. Through investigations, she identified enhancements to the bank's control environment. Sarah also worked previously in the forensic team at a Big 4 firm for 11 years, leading investigations into corporate and procurement fraud, embezzlement, bribery and corruption.

Sarah is a UK qualified chartered accountant, a certified fraud examiner and a certified anti-money laundering specialist.

FRA is an international consultancy specialising in regulatory cross-border investigations, compliance and litigation. We are regularly hired to support some of the world's largest multi-jurisdictional investigations and compliance matters and are consistently recognised as a global market leader. In over 20 years of supporting clients, we have assisted major multinational companies around the world from various sectors, including Airbus, Alstom, Telia Company, Total, HP, Société Générale and Rolls-Royce. We build strong relationships with our clients, acting as partner, trusted adviser and thought leader.

Unlike traditional accounting firms, we operate purely in the forensic space. We have experience working in more than 75 jurisdictions based in our 11 global offices and data centres across the United States, United Kingdom, France, Finland, Sweden, Canada and Switzerland. FRA's 'one firm' culture allows us to offer clients in any jurisdiction the best of our international expertise. Our globally integrated team of experts includes experienced forensic accountants, financial analysts, former investment bankers, attorneys, software engineers and certified computer examiners.

Our core areas of expertise are forensic accounting, data analytics and data governance, technology solutions and forensics. We advise international companies in all areas of white-collar crime and fraud, from preventive compliance activities to enforcement responses, investigations and post-enforcement compliance improvements. To assist our clients in achieving their objectives in the most sensitive and complex matters, we offer extensive multi-jurisdictional data privacy, transfer and protection expertise. Where data cannot be moved outside of a host country, our full-service Mobile Discovery Solution offers a scalable end-to-end mobile processing and review platform.

Audrey House
16-20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 020 7831 9110
www.forensicrisk.com

Deborah Luskin
dluskin@forensicrisk.com

Anant Modi
amodi@forensicrisk.com

Selma Della Santina
sdellasantina@forensicrisk.com

Sarah Wrigley
swrigley@forensicrisk.com

As well as daily news, *GIR* curates a range of comprehensive regional reviews. This volume, the *Europe, Middle East and Africa Investigations Review 2020*, contains insight and thought leadership from 32 pre-eminent practitioners from these regions. Inside you will find chapters on France, Germany, Italy, Nigeria, Romania, Russia, Switzerland and the UK (from multiple angles), the new fronts in fight against money laundering, how to 'remediate' in Africa – and lots more.

Visit globalinvestigationsreview.com
Follow @GIRAlerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-269-5