GIR INSIGHT

EUROPE, MIDDLE EAST AND AFRICA INVESTIGATIONS REVIEW 2021

EUROPE, MIDDLE EAST AND AFRICA

INVESTIGATIONS REVIEW 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
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: 978-1-83862-594-8

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

Contents

Preface

Welcome to the *Europe, Middle East and Africa Investigations Review 2021*, 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 the exigencies of journalism allow.

The *Europe, Middle East and Africa Investigations Review 2021*, which you are reading, is part of that series. It contains insight and thought leadership from 30 pre-eminent practitioners around these regions.

All contributors are vetted for their standing and knowledge before being invited to take part. Together they capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. The result is a book that is an invaluable horizon scanning tool.

This edition covers France, Germany, Italy, Romania, Russia, Switzerland and the UK; and has overviews on trends in anti-money laundering; compliance programmes in Central and Eastern Europe; and how to conduct a root cause analysis in Africa, with the aid of a hypothetical case study.

As so often is the case with these annual reviews, a close read yields many gems. On this occasion, for this reader they included that:

- 2019 was the first year that EU anti-money laundering fines exceeded the US's (on both volume and value);
- there are four distinct ways to organise a root cause analysis;
- covid-19 has led most governments in Central and Eastern Europe to disregard their public procurement rules;

- Romania is cracking down on bribery in healthcare and it would appear 11 of the 20 largest pharma companies operating there are implicated;
- Russia continues to distinguish between attorneys and advocates when it comes to legal privilege, which is never secure at the best of times (so if you want the best chance at invoking it – make sure you hire an advocate!); and
- the UK FCA is showing far greater interest in the area of 'non-financial misconduct', posing all sorts of investigative challenges.

Plus many, many nuggets of not previously known information.

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 2021

Anti-Money Laundering Trends and Challenges

Charlie Steele, Sarah Wrigley, Selma Della Santina and Deborah Luskin
Forensic Risk Alliance

In summary

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations continue to increase year on year. Regulators are active globally, and AML penalties in Europe have exceeded those in the United States in recent years. To provide context for financial institutions and companies preparing for Europe's strengthening AML enforcement, this article traces the changing regulatory environment, recent challenges and typology trends. The article discusses the push towards AML 'effectiveness' and highlights key elements that should be present in a robust AML programme.

Discussion points

- Significant advances have been made in EU money laundering legislation but with varying levels of implementation
- The United Kingdom is no longer required to implement EU AML rules but is likely to continue to match or exceed them
- Some new US rules may exceed those in the EU and affect EU entities
- There are growing calls for evaluating whether AML efforts are proving effective or merely increasing compliance costs

Referenced in this article

- EU Anti-Money Laundering Directives
- Identifying ultimate beneficial owners
- Virtual currencies
- Digital identity
- Trade-based money laundering
- Public–private and Private–Private information-sharing partnerships
- US Federal Financial Institutions Examination Council's key elements to an AML programme

Introduction

Enforcement actions and penalties for non-compliance with anti-money laundering (AML) regulations continue to increase. Globally, there were 58 AML penalties in 2019 totalling US$8.14 billion, compared to 29 penalties totalling US$4.27 billion in 2018. This was almost a doubling of fines within one year. In 2020, global AML fines for financial institutions increased again to more than US$10.3 billion.[1]

Historically, US AML penalties dwarfed other regions, but that is no longer the case. Regulators are active globally, and the largest penalties in any given year have been different in each of the past few years. In 2019, European authorities exceeded US-ordered AML penalties, totalling US$5.8 billion against US$2.2 billion.[2] In 2020, the Asia-Pacific exceeded US-ordered AML enforcement actions for the first time since 2015, totalling US$5.1 billion against US$4.3 billion,[3] largely against Goldman Sachs in relation to 1MDB, and Westpac in relation to transaction monitoring and reporting failures for serious crimes.[4]

To provide context as financial institutions and companies plan their responses to the continued strengthening of AML enforcement in Europe, this article describes the changing regulatory environment, recent challenges and typology trends. We also discuss the push towards AML 'effectiveness' and what that means for regulators and financial institutions. Finally, we highlight the key elements that should be present in a robust AML programme.

Regulatory changes

European Union

There have been signficant advances in money laundering legislation within the European Union, but with varying levels of implementation. A series of Anti-Money Laundering Directives (AMLDs) were passed between 1991 and 2020, the most recent of which included the Fifth AMLD (5AMLD) and the Sixth AMLD (6AMLD).

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 European Union unless the jurisdictions have comparable AML regimes;
- made ultimate beneficial owner (UBO) lists public within 18 months;
- mandated functional public politically exposed persons (PEP) lists; and
- mandated enhanced due diligence measures to monitor transactions with high-risk countries.

1 www.fenergo.com/press-releases/global-financial-institution-fines-for-aml-data-privacy-and-mifid-rise-26-in-2020/.

2 Ibid.

3 www.complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article.

4 www.regulationasia.com/lessons-learned-from-apacs-landmark-year-of-aml-fines/.

The 6AMLD focuses on aligning 22 predicate crimes, extends criminal liability to legal persons and increases the maximum term of imprisonment from one to four years.

There have been and continue to be two layers of inconsistency in AML efforts within the European Union. First, AMLDs must be transposed into national law. However, the timeliness of that transposition has been patchy. For example, in February 2020, the EU Commission sent letters of formal notice to eight EU countries for not having notified any implementation measures for the 5AMLD, which was updated more than two years prior and had a January 2020 deadline.[5] Even more concerning, in 2021, the EU Commission sent letters of notice to Germany, Portugal and Romania for incorrectly transposing the Fourth Anti-Money Laundering Directive (4AMLD), which had a transposition deadline in June 2017.[6]

Second, there have been a series of AML rule breaches in European banks, which has raised doubts about the effectiveness of EU bank supervision. In some recent AML scandals, country supervisors only took action after the US Financial Crimes Enforcement Network (FinCEN) took special measures[7] or investigative journalists uncovered wrongdoing.[8] The European Banking Authority (EBA) published a report that evaluated the effectiveness of member state AML supervision and identified several areas of supervisory weakness, including: not assessing control effectiveness versus confirming a prescriptive set of requirements; not taking proportionate and sufficient dissuasive measures; and not working effectively with domestic and international stakeholders.[9]

To address the well-publicised regulatory failures and inconsistencies in EU AML regulation, in November 2020, the EU Council formally agreed to create an EU-wide AML regulator with direct authority to review and penalise institutions.[10] The Council supports the creation of an EU-level supervisor that has direct supervisory powers over a select number of obliged high-risk entities, as well as authority to take over supervision from a national supervisor in clearly defined and exceptional situations.

In addition, the Council is prioritising proposals to implement AML rules via EU Regulations (as opposed to EU Directives), which would not require transposition into national law, and a mechanism for better coordination between EU financial intelligence units (FIUs). These various proposals will likely start to take shape in 2021.

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

6 https://ec.europa.eu/commission/presscorner/detail/en/inf_21_441.

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

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

9 'EBA Report on Competent Authorities' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks', European Banking Authority (published 5 February 2020).

10 www.consilium.europa.eu/en/meetings/ecofin/2020/11/04/.

United Kingdom

The United Kingdom is no longer required to implement EU AMLDs; however, it is likely that the UK AML legislation will continue to match, or exceed, AML rules set by the European Union.

The primary AML legislation in the United Kingdom is set out in: the Proceeds of Crime Act 2002; the Terrorism Act 2000; the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; and the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. A review of AML legislation is currently being carried out as part of the Economic Crime Plan 2019–2022, with proposals related to information sharing, the suspicious activity reporting (SAR) regime and AML effectiveness.[11]

The United Kingdom is active in AML enforcement. In addition to the US$50 million penalty of the Financial Conduct Authority (FCA) against Commerzbank, the FCA and the Prudential Regulation Authority jointly fined Goldman Sachs US$126 million for risk management failures relating to 1MDB.[12] The FCA has recently commenced the first criminal prosecution of a bank – against Natwest – for money laundering.[13]

United States

The primary legislation in the United States governing AML has grown over time, from the Bank Secrecy Act of 1970 (BSA) to the Money Laundering Control Act of 1986 and sections within the US PATRIOT ACT of 2001. There have also been smaller updates, such as the inclusion of virtual currency providers in 2013 and the Customer Due Diligence Rule requiring verification of customers in 2016.

At the end of 2020, the United States passed a series of acts with significant changes and enhancements to the AML rules. Some of those new rules, such as a national beneficial owner registry and whistle-blower protections, bring the United States in line with existing EU rules.

In contrast, some of the new rules exceed those in the European Union and may affect EU entities. One example is the increased penalties enacted under the Anti-Money Laundering Act (AMLA). They include prohibitions on knowingly concealing or misrepresenting a material fact from or to a financial institution concerning ownership or control of assets for PEPs or misrepresenting a material fact concerning the source of funds in a transaction that involves an entity that is a primary money laundering concern.[14] The penalties for violating those rules are up to 10 years' imprisonment or a US$1 million fine, or both.

Another example is the increased authority to seek documents from non-US financial institutions. Previously, those subpoenas could be issued to any non-US bank that maintained a correspondent account in the United States, but could only request records related to the specific correspondent account.

11 www.rusi.institute/ecp/.

12 www.fca.org.uk/news/press-releases/fca-pra-fine-goldman-sachs-international-risk-management-failures-1mdb.

13 www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc.

14 AMLA 2020, §5335.

The new statute expands this authority to allow the US Department of Justice to seek 'any records relating to the correspondent account or any account at the foreign bank, including records maintained outside of the United States', if the records are the subject of an investigation that relates to a violation of the BSA, a violation of US criminal laws, a civil forfeiture action, or a primary money laundering concern investigation (as applied to ABLV Bank in Latvia in 2018). Essentially, the subpoena powers have expanded from the specific correspondent account to any account at the non-US bank if the requested records fall within one of those investigative categories.

Further, if the non-US financial institution fails to comply, the Act authorises the US Treasury to direct the related US financial institution to terminate the correspondent banking relationship, as well as impose penalties.[15]

Virtual currencies

Timothy Massad, former chair of the US Commodity Futures Trading Commission, has written extensively about crypto-asset oversight, stating: 'The basic, overarching issue is that digital asset innovation has outpaced our regulatory framework.' There is reason to think that regulators are working hard to catch up.

In October 2018, the Financial Action Task Force (FATF) modified their recommendations to clarify that they apply to virtual assets (VAs), and that virtual asset service providers (VASPs) should be regulated, licensed or registered and subject to effective systems for monitoring or supervision. In June 2019, the FATF issued guidance[16] with specific points for regulating digital assets and associated exchanges.

It is a fast-moving area of regulation with a large number of regulatory proposals in various jurisdictions around the world. In July 2020, the FATF published a 12-month follow up regarding regulatory oversight of virtual assets.[17] At the time, 35 out of 54 reporting jurisdictions said they had implemented the revised 2018 standard. The other 19 jurisdictions had not yet implemented the revised standards in their national law.

The 5AMLD already requires virtual asset firms and exchanges to apply AML measures, including enhanced know-your-customer (KYC) programmes and reporting obligations. In September 2020, the EU Commission proposed new legislation – the Regulation of Markets in Crypto-Assets (MiCA) – which aims to create a single licensing regime across all EU member states and streamline virtual asset regulation in the European Union for currently out-of-scope crypto-asset types, such as stablecoins and crypto-asset service providers, a term that encompasses more service types.

15 AMLA 2020, §6308.

16 www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

17 www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

Questions remain regarding the applicability of AML regulations to private wallets and peer-to-peer transactions. In December 2020, FinCEN released a notice of proposed rule-making that would include unhosted wallets in BSA requirements.[18] There has been a strong negative reaction to the proposed rule. Virtual asset exchanges complain that it is an undue burden, and many people are concerned about the privacy implications because once an unhosted wallet has been identified on a public blockchain, every transaction ever made by that wallet can be easily traced.

In February 2021, the FATF agreed to seek public consultation on previous guidance for AML obligations in relation to VAs and VASPs. It has indicated that future guidance will clarify some of the more challenging aspects of regulation in regard to virtual currency, such as stablecoins, the travel rule implementation and how to address the risks of peer-to-peer transactions.

AML Challenges

Identifying ultimate beneficial owners

A critical component in combating money laundering, and a regulatory expectation, is understanding who your customer is and who the UBOs are and the nature of their business. Determining the UBO is notoriously difficult, especially when customers provide false information or use corporate vehicles in secrecy havens. Even when those lists are made available, such as with the United Kingdom's Companies House, the information provided is not consistently verified.[19, 20]

When compliance personnel attempt to verify customer-provided UBO information, it can be a timely and costly process. Until 2020, most countries did not publish free, public ownership registers, so the information provided to financial institutions was more difficult to verify. The 5AMLD mandates publicly accessible UBO registers, but many member states have either not established those registers or not made them publicly available.[21, 22]

In February 2021, Transparency International led a group of 700 signatories calling on the UN General Assembly to set standards for transparency of beneficial ownership, specifically asking all countries to establish public registers of companies with the names of UBOs.[23]

18 Virtual currency wallet where the owner's private keys are not held by a financial institution, also called 'peer-to-peer'.

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

20 'Companies House regime faces major overhaul', Accountancy Daily (www.accountancydaily.co/companies-house-regime-faces-major-overhaul).

21 www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/5amld-patchy-progress/.

22 https://medium.com/transparent-data-eng/ultimate-beneficial-owners-registers-in-the-eu-2020-5a868e3ff0.

23 www.transparency.org/en/press/ungass-2021-hundreds-join-petition-to-end-anonymous-shell-companies#.

Leveraging technology

There is a regulatory expectation that institutions monitor customer activity to identify suspicious patterns or behaviour. This can only be achieved when an institution effectively aggregates its data across systems, divisions and geographic locations. However, transactional data is often held in different repositories (eg, card services and deposit operations) and in numerous legacy systems owing to previous acquisitions. If the disparate data could be analysed as a group, it would likely improve the ability to identify potentially unusual transactional activity.

AML detection is often automated, but generally not predictive. If a machine learning (ML) 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 have been encouraging innovative approaches, such as artificial intelligence (AI) and ML, to more effectively identify suspicious activity. A joint statement issued by various US regulators in December 2018 encouraged the use of internal financial intelligence units devoted to identifying complex illicit finance threats and experimenting with AI and digital identity technologies.[24]

Utilising digital identity

Two key drivers in digital identity are becoming more prominent. The first is that of the estimated 2 billion unbanked adults worldwide, 360 million are unable to access the formal financial sector owing to insufficient identity documentation.[25] The second is that non-cash transactions grew last year by the highest rate in the past decade,[26] and this trend is expected to continue.[27] Digital identity has the potential to provide a high level of assurance regarding identification while protecting privacy. It can be provided through a government, such as eID in Estonia and Lithuania, or a financial institution, such as BankID in Sweden and Norway.[28]

As noted in the FATF's Digital Identity guide,[29] digital ID verification systems present several risks, including identity theft, forged or tampered source documents, misuse of data owing to unauthorised access and the potential for data theft when communicating via the Internet. It is estimated that synthetic identity fraud, where criminals use fake IDs to secure credit, is the fastest-growing type of financial crime in the United States and costs lenders an estimated US$6 billion annually.[30]

24 'Joint Statement on Innovative Efforts to Combat Money Laundering', FinCEN (published 3 December 2018). Issued by the US Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration and the Office of the Comptroller of the Currency.

25 http://documents1.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf.

26 https://worldpaymentsreport.com/wp-content/uploads/sites/5/2020/10/World-Payments-Report-2020.pdf.

27 www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/accelerating%20winds%20of%20change%20in%20global%20payments/2020-mckinsey-global-payments-report-vf.pdf.

28 www.enisa.europa.eu/publications/eidas-compliant-eid-solutions.

29 www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

30 www.thomsonreuters.com/en-us/posts/corporates/synthetic-identity-fraud/.

Regulators have implemented rules regarding reliance on digital identity verification. The 5AMLD states that an obliged entity must identify the customer, which can be based on traditional documentary evidence or information obtained from a reliable and independent source, including electronic identification means.[31] Those electronic identification methods must comply with Regulation (EU) No 910/2014, which sets out criteria for identity verification services.[32]

The United Kingdom's Joint Money Laundering Steering Group indicates that digital identification may provide satisfactory evidence of identity on its own, but it must use data from multiple sources and across time, or incorporate qualitative checks that assess the strength of the information supplied, or it must be performed through an organisation that meets the EU criteria referenced above.[33]

Recent typology trends

As with most types of crime, when one money laundering method becomes more challenging to execute, perpetrators will devise 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 five 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 non-bank financial sectors and businesses.[34]

Trade-based money laundering (TBML) is the process of disguising proceeds of crime and moving value through the use of trade transactions.[35] It is increasingly viewed as a point of high vulnerability in efforts to combat money laundering.[36] Of the three broad methods of money laundering (ie, using financial institutions, physically smuggling cash and using the international trade system), the FATF has found that the abuse of the international trade system has historically received relatively little attention.[37]

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

31 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN.

32 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN.

33 https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-I_-July-2020.pdf.

34 'Countering Illicit Finance and Trade: U.S. Efforts to Combat Trade-Based Money Laundering,' US Government Accountability Office (published 30 December 2019).

35 'Trade Based Money Laundering', page 5, FATF (published June 2006).

36 'Uncontained', *The Economist* (published May 2014).

37 'Trade Based Money Laundering', page 5, FATF (published June 2006).

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 transhipment points.

To counter TBML, companies must assess their risk and consider relevant red flags. Financial institutions must factor TBML into their risk assessments and implement sufficient controls for reviewing trade documentation supporting letters of credit and how they monitor payment messages for open trade transactions.[38]

In December 2020, the FATF issued updated guidance regarding TBML.[39] The report notes that the exploitation of TBML techniques is particularly effective when there is a complicit relationship between the importer and exporter, who are actively misrepresenting the trade or invoice process. It further notes that authorities can have a greater impact if they can disrupt these complicit actors through criminal prosecution or removing their authority to trade.

The report also highlights the use of third-party intermediaries linked to organised crime or professional money launderers. While financial institutions are often aware of risks in dealing with such third-party intermediaries, others in the supply chain, such as legitimate importers or exporters, or those with an oversight role such as auditors or accountants, may not question why an entirely unrelated third-party is involved in the payment settlement process.

Pandemic-related risk

Globally, there has been an increase in pandemic-related fraud, including counterfeit medical goods, cybercrime, investment fraud, charity fraud and abuse of economic stimulus payments. FATF released a report detailing these increased crimes in December 2020.[40] The paper documents changing financial behaviors, such as significant increases in online purchases due to widespread lockdowns and temporary closures of most physical bank branches.

FinCEN has issued a series of advisories regarding pandemic-related medical scams, including fraudulent tests and vaccines, non-delivery scams, price gouging of medical-related items, scams related to government payments and cybercrime.[41, 42, 43] They provide a number of potential red flags for financial institutions, including individuals selling medical equipment through personal accounts, selling highly sought-after goods at either deeply discounted or highly inflated prices, unusual payment terms for the medical industry, receipt of a document

38 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles, 2019 amendment.' the Wolfsberg Group (published 27 March 2019).

39 www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf.

40 www.fatf-gafi.org/publications/fatfgeneral/documents/updated-covid-19-ml-tf.html.

41 www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf.

42 www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

43 www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

that appears to be a check or prepaid debit card from the US Treasury at less than the expected amount, irregular digital identity documentation and customer logins from IP addresses in many jurisdictions within short time frame.

Ransomware

The use of ransomware is gaining in popularity and can be a method to launder money. According to the most recent CyberEdge Group survey, 62 per cent of organisations were victimised by ransomware in 2020, up from 56 per cent in 2018 and 55 per cent in 2017. The increase may be fueled by the dramatic increase in ransomware payments: 58 per cent paid the ransom in 2020, compared with 45 per cent in 2018 and 39 per cent in 2017.[44]

One of the 22 AML predicate offences that was harmonised across the European Union within the 6AMLD is cybercrime, which includes ransomware.[45] In October 2020, the European Union Agency for Cybersecurity issued a threat landscape guidance document regarding ransomware.[46] The document indicates that €10.1 billion was paid in ransom during 2019 – more than €3.3 billion higher than in 2018. They noted that 45 per cent of attacked organisations paid the ransom.

In October 2020, FinCEN issued an advisory for financial institutions regarding the increase in ransomware.[47] The advisory points out that financial institutions play a critical role in the collection of ransom payments. Ransom is most often paid via virtual currencies. The victim pays the perpetrator via a virtual currency exchange. The perpetrator then transfers the virtual currency, typically bitcoin, by transferring it many times via mixers and tumblers[48] to obscure the money trail or transferring the virtual currency to an exchange in a jurisdiction with weak AML controls.

Human trafficking and modern slavery

Human trafficking is one of the most profitable criminal enterprises, generating an estimated US$150 billion per annum.[49] Human trafficking from Africa and Asia into Europe is relatively well known, particularly where refugees from war-ravaged countries, including Syria, Iraq and Afghanistan, are exploited by traffickers for large sums and subjected to dangerous conditions.

Reports of modern slavery or forced labour in Europe are becoming more frequent and more high profile. For instance, a series of media reports exposed alleged modern slavery in the supply chain of companies such as the fashion retailer, Boohoo, which is now facing a potential US import ban.

44 https://cyber-edge.com/resources/2020-cyberthreat-defense-report/.

45 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.284.01.0022.01.ENG.

46 www.enisa.europa.eu/publications/ransomware.

47 www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

48 Services offered to mix potentially identifiable cryptocurrency funds with others to obscure the origin.

49 Estimate from the International Labour Organization.

FinCEN recently issued an advisory regarding human trafficking to supplement a previous advisory from 2014.[50] It points out that effects of the covid-19 pandemic, such as travel limitations, shelter-in-place orders and teleworking, may exacerbate the conditions that contribute to human trafficking and affect existing red flag indicators.

Since the previous advisory, it has identified an additional 10 financial and behavioural indicators of labour and sex trafficking, bringing the total to 20. It notes that human traffickers and facilitators have used front companies, exploitative employment practices, funnel accounts and alternative payment methods to facilitate money laundering. Some of the newly added red flags include frequent transactions with online classified sites based in foreign jurisdictions and frequently sending or receiving funds via cryptocurrency to or from darknet markets associated with illicit activity.

Illegal wildlife trade

The illegal wildlife trade is a major transnational organised criminal enterprise, generating criminal proceeds estimated at between US$7 and US$23 billion each year.[51] The covid-19 pandemic cast a new spotlight on this illicit activity owing to the zoonotic nature of the disease, which may have passed the covid-19 virus from animals to humans at a live animal market in China. Wildlife crime has been linked to drug, human and arms trafficking.

An FATF report from June 2020 noted that countries rarely investigate this crime and that neither governments nor the private sector have prioritised efforts to combat this risk.[52] The report states that criminals misuse the legitimate wildlife trade and other import or export businesses as a front to hide illegal proceeds from wildlife crimes. It also notes an increase in the role of online marketplaces and mobile and social media-based payments to facilitate the movement of proceeds from wildlife crimes.

In the European Union, environmental crime, including the illegal wildlife trade, is captured by the 6AMLD as a predicate offence to money laundering. This means that obliged entities should consider illegal wildlife trade in their risk assessment.

The push towards AML effectiveness

There has been a growing drumbeat over the past couple of years for evaluating whether global AML efforts have led to an appreciable reduction in predicate crimes and increased asset forfeiture, or merely increased compliance costs. Renewed focus on specific actions may lead to greater AML effectiveness, such as including risk-based procedures by both regulators and obliged entities, linking an obliged entity's risk assessment to national AML priorities, continuing to increase information sharing and leveraging technology.

50 www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf.

51 According to a 2016 UN report.

52 www.fatf-gafi.org/publications/methodsandtrends/documents/money-laundering-wildlife-trade.html.

FATF strategic review

This conversation regarding effectiveness versus mere implementation of rules picked up steam when the FATF announced in late 2019 that they had planned a strategic review of their evaluation process. At the time, David Lewis, the FATF Executive Secretary, stated that its evaluation of effectiveness had come to focus more on process than outcome. He added that the evaluation process was very effective in motivating countries to take action, but the motivation was generally to avoid a bad report rather than to reduce harm to society or protect the integrity of the financial system. He stated that the fourth round of FATF evaluations – the first to focus on effectiveness – showed that countries were taking a tick-box approach to regulatory compliance and focusing on processes rather than outcomes.[53]

In the June 2020 FATF Plenary, delegates agreed that the aim of future evaluations is to make them more timely, have a greater emphasis on effectiveness and strengthen the risk-based elements of the assessment process.[54]

What regulators can do differently

As the FATF February 2021 Plenary summary stated, transitioning from rules-based supervision to risk-based supervision takes time and can be challenging. It requires a change in supervisory culture where supervisors have an in-depth understanding of the risks that their regulated entities face.[55]

The FATF subsequently issued risk-based supervisory guidance in March 2021, which focuses on supervisors' understanding of risk and applying their strategy based on those risks.[56] This risk-based approach for supervision mirrors the FATF's own proposed approach to mutual evaluation reports going forward.

There are two key areas where regulators can take action to support greater effectiveness in countering money laundering. The first is helping financial institutions and other obliged entities develop their risk assessments by providing guidance to link the national risk assessment to those of the individual entities.

Detailed risk guidance, along with the entity's knowledge of its business, is useful to financial institutions and other obliged entities in helping to determine where their risk of money laundering is greatest and how they might mitigate those risks. The 4AMLD mandated that the European Commission conduct an assessment of money laundering and terrorist financing risks affecting the internal market and update it at least every two years.

53 www.fatf-gafi.org/publications/fatfgeneral/documents/rusi-fatf-strategic-review.html.

54 www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.

55 www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-february-2021.html.

56 www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf.

The most recent EU-wide risk assessment was published in mid-2019.[57] The risk assessment focuses on vulnerabilities at the EU level, both in terms of legal framework and effective application and provides recommendations for addressing the identified risks.[58] The description of money laundering risks within the European Union is relatively detailed; for example, within the gambling sector, it points out that land-based betting is high-risk owing to typically ineffective controls, whereas online gambling is high-risk owing to very large numbers of transactions and the lack of face-to-face interaction.

In addition, the 5AMLD mandated that EU member states make the results of their risk assessments available to the European Commission and the other member states, and make a summary version, without classified information, publicly available.

The second area where regulatory authorities can support effectiveness in AML efforts is providing specific feedback regarding suspicious transaction reports (STRs). The headlines surrounding the 'FinCEN Files' garnered a great deal of attention regarding the volume of STRs that did not appear to result in any action taken.

In fairness, it is unclear how individual STRs are collated with other information and considered by the respective FIU; however, most observers see an excessive amount of low-quality SARs being filed from a defensive position. The penalty for not filing an STR may be great, but there is no penalty for submitting a STR where it may not be warranted or is poorly written with little probative value.

What financial institutions can do differently

Some areas of improvement that would make financial institutions more effective in combating money laundering are not within their control, particularly the creation of complete and accurate UBO registers. However, there are two areas where financial institutions can take action: creating and maintaining risk assessments with proper governance and oversight; and information sharing.

The European Banking Authority recently issued revised guidance regarding risk factors for money laundering and terrorist financing.[59] Within those guidelines, it specifies that risk assessments should be performed at least annually or more frequently when necessary, and that they should always consider specific sources of information, including the European Commission's supranational risk assessment referenced above.

57 https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

58 https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

59 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf.

Within the United States, FinCEN has proposed new regulations to require obliged entities to conduct risk assessments and align their programmes with national priorities.[60] The stated purpose of the proposed amendment to require a risk assessment is to directly tie procedures to relevant risks and provide information with a high degree of usefulness to government authorities.

The second action financial institutions and other obliged entities can take in support of greater AML effectiveness is to participate in information sharing. 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. There is now an increasing trend of public–private partnerships and, in some cases, financial institutions sharing information directly with each other.

Examples of public–private partnerships

Netherlands

At the encouragement of the Dutch regulator, in 2019, four Dutch banks – ABN AMRO, ING, Rabobank and Volksbank – signed a covenant with the National Police and the FIU 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, which will compare it to their KYC and transaction data.

United Kingdom

The UK Joint Money Laundering Intelligence Taskforce (JMLIT) is a partnership between law enforcement and financial institutions for the exchange of 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 potentially suspicious behavior at an earlier stage

60 https://www.regulations.gov/document/FINCEN-2020-0011-0001.

Examples of private–private partnerships

Dutch banks

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 this information sharing can reduce costs and give compliance departments access to better, more timely KYC data.

Nordic banks

The five largest lenders in the Nordics – Danske Bank, DNB, Handelsbanken, Nordea and SEB – disclosed plans to share KYC data on large and medium-sized corporates with the goal of streamlining due diligence, similar to the initiative by the Dutch major banks.

TMNL

The Transaction Monitoring Netherlands (TMNL) partnership between five Dutch banks – ABN AMRO, ING, Rabobank, Triodos Bank and Volksbank – is operational and will begin joint monitoring of business payment transactions.[61]

Navigating legislation that requires protection of personal data presents challenges when private companies share information. However, some regulators are providing assurances regarding sharing such information in the AML context.

In December 2020, FinCEN published updated guidance[62] regarding information sharing, which gave financial institutions great latitude in sharing relevant information with each other. The guidance specified that the financial institution does not need to have specific information regarding proceeds of a crime, nor have made a conclusive determination that the related activity is suspicious, before sharing it. The guidance also stated that financial institutions can share information on attempted transactions and information that includes personally identifiable information, and that they are not restricted in their methods of sharing information, including verbally.

61 https://tmnl.nl/.

62 www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

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 owing to the reputational damage. Furthermore, remediation costs over the first 18 months are typically 12 times greater than the fine itself.[63]

Proactively addressing weaknesses in an AML compliance programme is a smart long-term proposition. The US Federal Financial Institutions Examination Council (FFIEC) has published a comprehensive inspection manual, which outlines the key elements of a BSA/AML programme.[64] The following table identifies key elements from the FFIEC manual and our suggested questions to guide your organisation's planning.

US FFIEC's key elements to a BSA/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 and geographies) and 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? • Does the risk assessment consider relevant national or supranational risk assessments? • Is there proper governance and oversight of the risk assessment process? • How often and under which circumstances is the risk assessment updated? • Has the risk assessment considered changes owing to the covid-19 pandemic, specifically differences in staffing and suspicious transaction reporting?
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 (CDD) policies, contain detailed procedures for STR, address segregation of duties and address the process for anomalous transaction reporting? • Are AML responsibilities included within job descriptions?

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

64 'BSA/AML Examination Manual', FFIEC (published 2014).

US FFIEC's key elements to a BSA/AML programme	Key questions for your organisation to consider
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? • Are the board of directors and executive management informed of their AML regulatory requirements?

Conclusion

AML risk management has become more challenging over time as the regulations have become more stringent. Financial institutions, in particular, have faced larger fines where compliance programmes have been deficient.

However, there has also been more detailed guidance developed by government[65] and non-government[66] bodies to help build a robust AML programme, technology developed to help entities become increasingly sophisticated in their ability to detect and monitor suspicious transactions, and partnerships formed to share information that enables a more comprehensive compliance effort.

When evaluating their compliance efforts, entities should be proactive and develop a robust AML compliance programme, paying particular attention to, for example, the CDD, UBO and transaction-monitoring elements. As part of this effort, entities must: keep up to date on changes to legislation and regulations; consider new and evolving technologies and typologies in the overall AML and counterterrorism financing risk assessment; where possible, share information in furtherance of a more comprehensive solution to identifying money laundering; and understand where efforts should be focused to work towards greater effectiveness in combating money laundering.

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

66 'Sound management of risks related to money laundering and financing of terrorism', Basel Committee on Banking Supervision (published 7 June 2017).

Charlie Steele
Forensic Risk Alliance

Charlie Steele is a partner in FRA's Washington, DC office with more than 30 years of government and private-sector experience in civil and criminal compliance, investigations, enforcement and litigation matters in a variety of industries and sectors. In recent years, he has specialised in economic sanctions and Bank Secrecy Act and anti-money laundering (BSA/AML) matters.

He is a former senior US Treasury Department and Department of Justice official, serving most recently as Chief Counsel for the Office of Foreign Assets Control (OFAC). In that role, he led the team of lawyers providing legal advice and support to OFAC and other Treasury Department personnel in the formulation, implementation and enforcement of economic sanctions.

Charlie has also served in a number of other senior positions in the Treasury Department: Associate Director for Enforcement in OFAC, Deputy Director of the Financial Crimes Enforcement Network (FinCEN, the US government's principal BSA/AML agency and the US financial intelligence unit) and Deputy Chief Counsel in the Office of the Comptroller of the Currency (the US supervisor and regulator of national banks).

Charlie earned his JD from the Georgetown University Law Center and has a BA in economics from the University of Virginia.

Sarah Wrigley
Forensic Risk Alliance

Sarah Wrigley is a director based in FRA's London office. She has over 18 years' experience in complex, cross-jurisdictional investigations, including financial crime and sanctions, regulatory issues and accounting irregularities. She has worked across a range of industries, with a focus on financial services.

Prior to joining FRA, Sarah was the Africa and Middle East Regional Head of Financial Crime Intelligence and Investigations for Standard Chartered Bank. Sarah led the bank's investigation response in the region to global financial crime issues generating media and regulatory scrutiny. 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.

Sarah previously spent 11 years in the forensic accounting team of a Big Four firm and has led investigations into corporate and procurement fraud, embezzlement, regulatory breaches, accounting misstatements and bribery and corruption. Sarah is a UK-qualified chartered accountant, a certified fraud examiner and a certified anti-money laundering specialist.

Selma Della Santina
Forensic Risk Alliance

Selma is a director based in FRA's Zurich office. She has over 13 years of experience in forensic accounting, financial due diligence and auditing. She specialises in responding to regulatory enforcement requests in the financial services industry. Selma has extensive experience in leading large international teams in various financial crime and tax transparency investigations. She also has significant experience in 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.

Prior to joining FRA, Selma worked at EY and PwC in Australia, Austria, Slovenia and Switzerland. During her tenure, she gained extensive experience in leading large international teams to investigate, remediate and assess financial crime infractions, working alongside in-house investigations teams and external legal counsel. She also has a deep understanding of complex client structures in Swiss private banking, as well as of local and the international regulatory environment relating to financial crime topics.

Selma is a certified fraud examiner and holds a Master of Business Administration. She is also an ETHIC Intelligence certified ISO 19600 and ISO 37001 certified auditor. She is fluent in English, Italian, Bosnian and Slovene.

Deborah Luskin
Forensic Risk Alliance

Deborah Luskin is an associate director in FRA's Washington, DC office with over 19 years' experience in auditing and consulting. Deborah has experience in forensic accounting, financial audit attestation, risk management assessments, Sarbanes-Oxley 404 readiness and audit attestation and service organisation internal control assessments.

While at FRA, Deborah has focused on regulatory reviews and anti-financial crime projects, including assisting companies in responding to regulatory enquiries, investigating potential non-compliance with anti-money laundering (AML) regulations, assessing AML and sanctions compliance programmes, developing risk assessments, drafting policies and procedures, and providing guidance regarding customer due diligence procedures.

Prior to joining FRA, Deborah spent nine years at a Big Four firm working in risk management. Deborah specialised in assessing both financial and information systems internal controls, supporting the financial statements, assessing regulatory compliance, performing fraud evaluations and assessing risk management programme effectiveness. Deborah led large multinational teams in various industries.

Deborah is a certified public accountant, a certified anti-money laundering specialist, a certified global sanctions specialist, a certified fraud examiner, a certified information systems auditor and a certified information systems security professional. She is also certified in financial forensics.

Forensic Risk Alliance (FRA) is a forensic accounting, data governance and compliance consultancy firm specialising in international corruption and fraud investigations for major global corporations and law firms. For more than 20 years, FRA has offered extensive multi-jurisdictional data privacy, transfer, and protection expertise to help clients achieve their objectives with compliance, litigation and investigations. With over 170 employees, FRA is headquartered in London – one of 10 locations across Europe, the Middle East and Africa and the United States. FRA has extensive cross-sector and cross-border experience and scalability anywhere in the world, with globally integrated teams across both developed economies and emerging markets, having worked in more than 75 countries and with the capability to speak over 30 languages.

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

Charlie Steele
csteele@forensicrisk.com

Sarah Wrigley
swrigley@forensicrisk.com

Selma Della Santina
sdellasantina@forensicrisk.com

Deborah Luskin
dluskin@forensicrisk.com

As well as daily news, *GIR* curates a range of comprehensive regional reviews. This volume contains insight and thought leadership from 30 pre-eminent practitioners in Europe, the Middle East and Africa. Inside you will find chapters on France, Germany, Italy, Romania, Russia, Switzerland and the UK, plus overviews on the fight against money laundering, compliance around Central and Eastern Europe and how to conduct a root cause analysis in Africa.

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

ISBN 978-1-83862-594-8