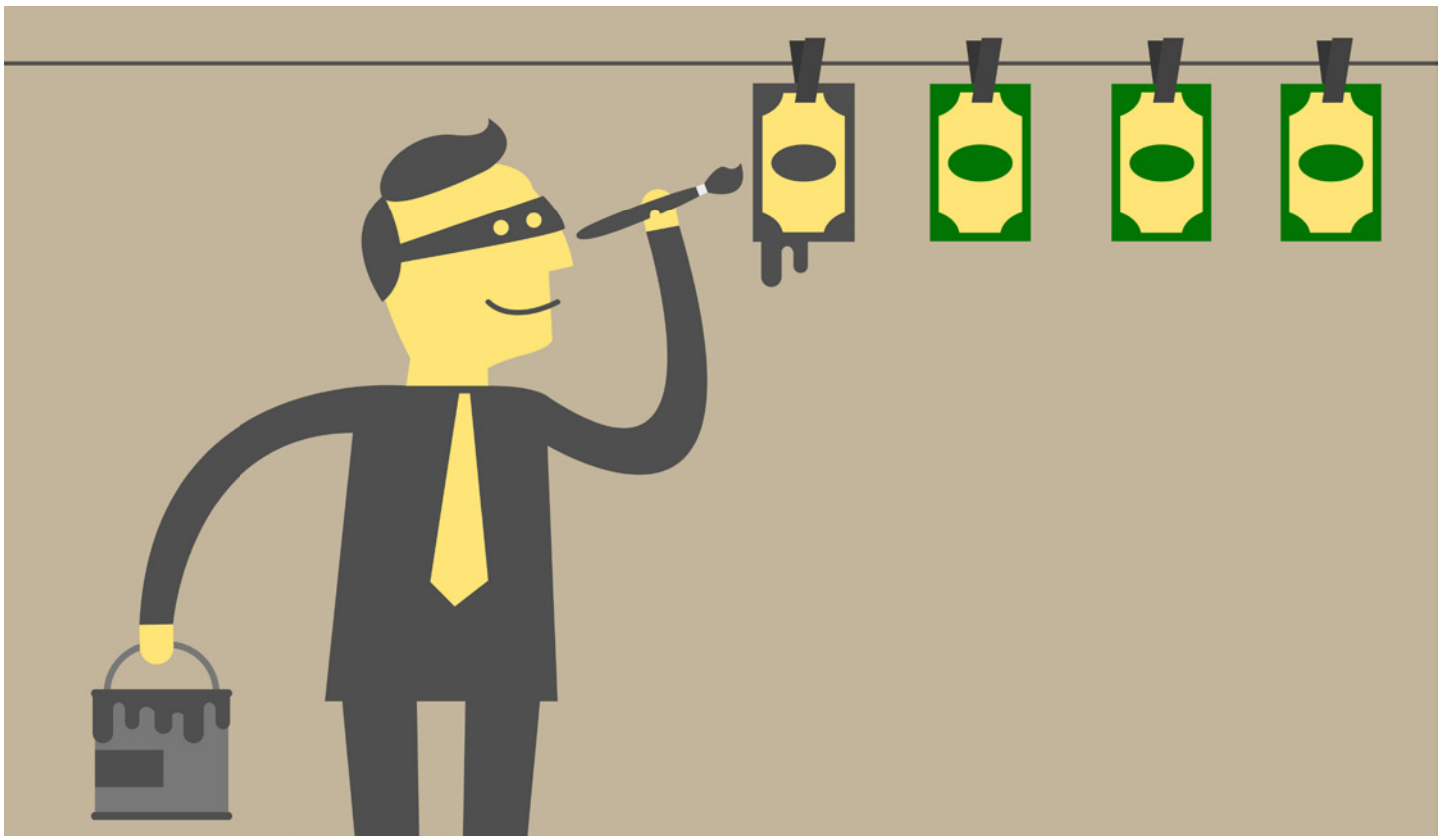
ROUNDTABLE July 2022

ANTI-MONEY LAUNDERING TRENDS

Despite efforts by authorities to detect and combat money laundering, such crime continues to plague global economies, with an estimated 5 percent of GDP laundered each year, approximately $2 trillion. In addition, asset management has become increasingly virtual, which has allowed money launderers to adapt their methods accordingly. This, in turn, puts pressure on regulatory bodies, and the financial services sector as a whole, to ensure their AML controls are sufficiently robust to deal with complex and evolving money laundering typologies. ■



THE PANELLISTS

Abhishek Dawar
Director, Arendt Regulatory and Consulting (ARC)
T: +352 40 7878 9355
E: abishishek.dawar@arendt.com
www.arendt.com

Abhishek Dawar is a director in the anti-money laundering (AML) and counter-terrorist financing (CTF) practice of Arendt Regulatory and Consulting (ARC). He is a skilled financial crime compliance expert with 14 years' experience, with a particular focus on delivering large-scale, complex financial crime compliance (FCC) programmes for the banking and asset management industries across multiple jurisdictions, including Luxembourg, the UK, Ireland, Gibraltar, the Isle of Man, Iceland, Sweden, Denmark, Norway, Finland, Belgium and India. He is also a tech-savvy professional, with broad expertise designing, implementing and testing FCC frameworks and target operating models for AML and sanctions.

Joydeep Sengupta
Counsel, Mayer Brown
T: +33 6 8966 0102
E: jsengupta@mayerbrown.com
www.mayerbrown.com

Joydeep Sengupta is a member of the compliance, investigations and regulatory team of Mayer Brown's Paris office, within the litigation and dispute resolution department. He focuses on cross-border litigation, compliance and enforcement matters for financial institutions and corporations, including the resolution of administrative and enforcement proceedings involving regulators and prosecutors. He has represented major US and European banks as well as global corporations in internal investigations related to US and European anti-money laundering, economic sanctions, market manipulation and anticorruption laws. He has conducted internal investigations around the world, including in France, Japan, Italy, Singapore, Spain, Switzerland, UK and the US.

Nabeelah Begum
Financial Crime Manager, Norton Rose Fulbright LLP
T: +44 (0)20 7444 2085
E: nabeelah.begum@nortonrosefulbright.com
www.nortonrosefulbright.com

Nabeelah Begum is a financial crime manager based in London. She focuses on anti-money laundering (AML), due diligence, counter-terrorist financing (CTF), economic and trade sanctions, proliferation financing and anti-corruption/anti-bribery. She has a wealth of industry and consulting experience, and her client coverage includes leading retail, commercial and investment banks, and wealth and asset management firms. She has a proven capability of successfully leading and delivering complex and regulatory critical programmes, as well as providing advisory services specifically in relation to financial crime compliance.

Eric Russo
Partner, Quinn Emanuel Urquhart & Sullivan, LLP
T: +33 (0)1 74 31 35 20
E: ericrusso@quinnemanuel.com
www.quinnemanuel.com

Eric Russo joined Quinn Emanuel Urquhart & Sullivan, LLP in 2021. Formerly a first deputy financial prosecutor at the PNF, his practice focuses on white-collar crime, regulatory investigations, compliance and litigation. He advises and assists companies and their managers around the world in the conduct of internal investigations and, in the context of judicial investigations, at all stages of the criminal proceedings from the opening of the investigation to the trial, including extradition and European arrest warrant proceedings. His expertise also covers financial market abuses and corporate and commercial litigation.

Eytan J. Fisch
Partner, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
T: +1 (202) 371 7314
E: eytan.fisch@skadden.com
www.skadden.com

Eytan J. Fisch has extensive experience representing global financial institutions and multinational companies on complex cross-border compliance and enforcement matters, including internal investigations, voluntary disclosures, and administrative and enforcement proceedings. He frequently counsels US and international clients on numerous aspects of US economic sanctions and anti-money laundering laws, including day-to-day compliance counselling, the development and implementation of compliance programmes, and issues that arise in the context of M&A.

FW: How would you characterise the prevalence of money laundering across the globe? How are recent innovations such as cryptocurrencies, virtual assets, and so on, changing the playing field?

Sengupta: From fine art to luxury yachts and crypto assets, the proceeds of crimes are continuously being laundered across borders, posing significant enforcement risks for financial institutions (FIs). The UN Office on Drugs and Crime (UNODC) estimates that 2-5 percent of global gross domestic product (GDP) is laundered annually – between $800bn and $2 trillion. The challenges of enforcing recent Russian sanctions has also revealed the difficulty of tracing proceeds of corruption spread across high-value assets in multiple jurisdictions offering anonymity and barriers to traceability, including luxury real estate and yachts owned by offshore trusts and other high-value assets that can be transferred easily, such as art, precious stones, jewellery and watches. Increased anti-money laundering (AML) prevention, detection and enforcement has, in turn, resulted in greater technological sophistication and layering, as well as continued use of complex offshore corporate structures. Cryptocurrencies and virtual assets have certainly offered new laundering vehicles greater anonymity.

Russo: Despite critical efforts from authorities to enhance their ability to detect and combat money laundering around the world, criminals have shown their great capacity for reinvention. Asset management has become increasingly virtual, which has allowed money launderers to adapt their modus operandi accordingly. As an example, Chainalysis detailed in its 2022 'Crypto Crime Report' that criminals have laundered $8.6bn worth of cryptocurrency in 2021, representing a 30 percent increase compared to 2020. With the emergence of FinTech start-ups, new payment methods and virtual currencies, new vectors allowing for money laundering are less heavily regulated and easily accessible, making them perfect targets for financial criminals. Neobanks have recently been particularly criticised because of deficiencies in their financial crime controls. This was exemplified with the investigation carried out by the UK Financial Conduct Authority (FCA) against N26, where it has been reported that AML failures were identified. Cryptocurrencies are difficult to trace, which facilitates placement and layering operations and makes of them a convenient tool for money laundering.

Dawar: Money laundering has been prevalent for many years. Large sums of money are laundered every year, posing a significant threat to the global economy and its security. As per various studies and regulatory trends, financial crime has thrived during the coronavirus (COVID-19) pandemic. For example, corruption is one of the primary drivers for money laundering and during the pandemic many such cases have been seen. With traditional fiat money, tackling money laundering was already a challenge, and with recent innovations such as cryptocurrencies and virtual assets, the playing field has drastically changed. If we look at recent examples of ransomware attacks and darknet markets, accepting funds in cryptocurrencies remains the preferred mode of payments for criminals. The varying level of crypto regulations across the globe and the decentralised nature of the cryptocurrency ecosystem has aggravated the problem and made it difficult for authorities and compliance professionals to detect and fight criminal activity.

Fisch: Reports from both the private sector and US government agencies consistently highlight that money launderers' ability to conceal criminal activity and the impact this has on the global financial system remain a significant concern. Innovation in the virtual asset space has been a focus of government with respect to money laundering risks. While the pace of development and innovation certainly poses challenges in assessing how to fit novel financial products and payment rails into existing regulatory and compliance frameworks, innovation also offers opportunities from a compliance standpoint. One example is the inherent immutability of transactions on the blockchain, which allows financial intelligence units and law enforcement to more effectively track and trace the proceeds of criminal activity as they move through the financial system. For instance, in February of this year, the US Department of Justice (DOJ) and the US Department of the Treasury's Internal Revenue Service announced the recovery of more than $3.6bn of the $4.5bn in bitcoin that was stolen in 2016 from Bitfinex, a virtual currency exchange. Law enforcement's ability to follow the digital breadcrumbs and recover these stolen funds also led to the arrest of two individuals involved in layering the stolen proceeds.

Begum: Money laundering continues to be one of the biggest threats to global society with it being estimated that around 5 percent of GDP is laundered each year, which translates to approximately $2 trillion. Cryptocurrencies and virtual assets are a key innovation during the past few years, and have had a large impact on money laundering globally as bad actors can use the anonymity associated with them as a way to conceal their illicit activities. Moreover, the new and unknown nature of cryptocurrencies and virtual assets has led to a rise in scams globally. This rise has put pressure on regulatory bodies, and the financial services sector as a whole, to make sure their AML systems and controls are robust enough to deal with the new offerings and the complex money laundering that results.

FW: What recent efforts have been made on the legal and regulatory front to combat money laundering? To what extent have authorities increased their anti-money laundering (AML) monitoring and enforcement efforts?

Russo: Reports from authorities show that recent AML enforcement frameworks have focused on targeting the emergent, increasingly sophisticated methods of money laundering. In France, the government presented its AML plan for action in March 2021. This plan sets

out five priorities for the next two years: detection, prevention, transparency, rigidity and coordination. In July 2021, the European Commission (EC) presented an extensive package of legislative proposals to strengthen the European Union's (EU's) AML and counter-terrorist financing (CTF) rules. Prominently, it includes the establishing of a new EU AML and CTF authority, a new EU regulation on AML and CTF containing directly applicable rules in EU member states, and a revision of the 2015/847/EU Regulation on Transfers of Funds to improving the tracing of crypto asset transfers. In October 2021, the Financial Action Task Force (FATF) published an updated guidance on AML requirements for virtual assets and virtual asset service providers, clarifying certain points in areas such as stable coins, peer to peer transactions, non-fungible tokens and decentralised finance. In February 2022, the DOJ announced its first director of the National Cryptocurrency Enforcement Team whose task is to investigate and prosecute criminal misuses of cryptocurrency. These recent moves from the AML authorities across the globe confirm that their attention has been increasingly focusing on virtual assets and cryptocurrencies, besides more traditional money laundering patterns that are still continuously monitored.

Dawar: In Luxembourg, there has been a notable increase in firms' AML and CTF resources, alongside more robust supervisory functions of the competent authorities. Moreover, despite authorities' longstanding proactive attitude toward enforcing legal and regulatory requirements, we have seen an increase in onsite visits to ensure procedures and controls have been implemented and are effective. These trends in Luxembourg are reflected in most European countries and stem from the European Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended, notably, by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as well as amending Directives 2009/138/EC and 2013/36/EU which have continuously promoted the collaboration between EU member states and national competent authorities (NCAs).

Fisch: In January 2021, the US enacted several significant pieces of legislation to strengthen and modernise the US AML and CTF legal framework, including the Anti-Money Laundering Act of 2020 and the Corporate Transparency Act. Several critical elements of these pieces of legislation have not been fully implemented. For instance, the US Treasury Department has yet to issue definitive regulations governing the highly anticipated beneficial ownership registry created by the Corporate Transparency Act, or the pilot programme under which participating FIs will be permitted to share suspicious activity reports (SARs) with their non-US affiliates. US regulators have also taken action to set higher compliance expectations. The New York State Department of Financial Services (NYDFS), for instance, recently published guidance on the use of blockchain analytics tools to enhance know your customer (KYC) and transaction monitoring capabilities in the virtual asset space. The US Treasury Department's Financial Crimes Enforcement Network (FinCEN) has similarly issued advisories regarding the money laundering-related risks posed by public corruption, and potential sanctions evasion risks surrounding designated Russian and Belarusian persons. US regulators and law enforcement agencies have remained active on the enforcement front, with an increased focus on the virtual asset industry. In addition to the Bitfinex enforcement activities, the DOJ secured guilty pleas from the founders of the Bitcoin Mercantile Exchange (BitMEX) for AML programme violations. FinCEN levied a $100m civil penalty against BitMEX for the violations in August 2021. The DOJ also recently announced the creation of Task Force KleptoCapture – an initiative dedicated to enforcing US sanctions imposed against Russia following its invasion of Ukraine, combatting efforts to circumvent US AML measures, and seizing assets tied to unlawful conduct through civil and criminal forfeiture mechanisms.

> "IT IS IMPORTANT FOR COMPANIES TO BE AWARE OF WHAT THEIR PEERS ARE DOING WITH RESPECT TO COMPLIANCE, GIVEN THAT MARKET STANDARDS EVENTUALLY HELP SHAPE REGULATORY EXPECTATIONS."
>
> EYTAN J. FISCH
> Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates

Begum: In the UK, the FCA and the Prudential Regulation Authority (PRA) have been taking strong and decisive measures to combat money laundering. There have been a series of 'Dear CEO' letters produced by the FCA and PRA,

with clear direction as to what the regulator expects and requires from firms. Furthermore, the Crown Prosecution Service (CPS) guidance in relation to the Proceeds of Crime Act 2002 (POCA) has been updated so that the CPS will now be able to prosecute individuals under section 330 of the POCA, regardless of whether it subsequently transpires that money laundering cannot be proven, or that it did not occur. In addition, the Law Commission has released a discussion paper seeking views on whether, and how, the law relating to corporate criminal liability can be improved. As a part of that paper, the Law Commission has sought views on a new corporate failure to prevent money laundering offences. All of this points to an increase in enforcement efforts to combat money laundering at all levels.

> TODAY, DESPITE PROGRESS MADE IN AML PROGRAMMES AND INCREMENTAL LEGAL AND REGULATORY OVERSIGHT, CERTAIN PRACTICAL ISSUES REMAIN IN HOW COMPLIANCE IS IMPLEMENTED.
>
> ERIC RUSSO
> Quinn Emanuel Urquhart & Sullivan, LLP

Sengupta: There have been significant recent legal developments on the AML front. The EU unveiled an AML and CTF legislative package in June 2021, setting out four legislative texts to harmonise EU AML laws. Topics addressed include the creation of a new AML/CTF body, enhanced customer due diligence (CDD), a beneficial ownership registry, enhanced cooperation between financial intelligence units (FIUs), and tracking crypto asset transfers. In the UK, the Economic Crime Act of 2022 creates a register of overseas entities and their beneficial ownerships, a register of real estate owned by overseas entities, enhances unexplained wealth orders and strengthens sanctions. In the US, following the US Anti-Money Laundering Act of 2020, in 2022, the Task Force KleptoCapture, the Kleptocracy Asset Recovery Initiative and the Kleptocracy Asset Recovery Rewards Program were created to enforce sanctions on Russian oligarchs. Enforcement is also rising in the UK, EU, US and Switzerland, with greater cooperation and information sharing between authorities.

FW: How intense is the pressure on companies to do more to counter financial crime? In your experience, do companies generally need to be more proactive about enhancing the due diligence and background checks they carry out on their business partners and customers?

Dawar: Regulatory pressure on firms is high and the sheer number of regulations that have been passed over the past four years is testimony to this. While AML and CTF legal and regulatory requirements remain complex and articulate, sanctions imposed by competent authorities on major FIs in Europe in response to recent money laundering and terrorist financing scandals demonstrates that firms have failed to comply with basic AML and CTF legal and regulatory requirements. When it comes to the identification of business partners or customers, there is definitely room for improvement. For example, the definition of beneficial owners and the way laws and regulations are applied by firms leaves loopholes that can be exploited by money launderers. When facing difficulties in identifying beneficial owners or in cases where red flags cannot be discounted, firms should consider going beyond classic KYC checklists to embrace forensic experts. Giving such experts access to relevant information can provide firms with value in the context of their due diligence, enabling them to have a better understanding of customers.

Fisch: There is constant pressure on the private sector to do more to combat financial crime. And as the marketplace evolves, so too do regulatory expectations regarding what constitutes effective and meaningful financial crime compliance. It is important for companies to be aware of what their peers are doing with respect to compliance, given that market standards eventually help shape regulatory expectations. The guidance issued by NYDFS regarding the use of blockchain analytics tools is one example of how innovation and market trends have led to new or heightened expectations regarding customer due diligence and transaction monitoring controls. For these reasons and others, the more proactive companies can be in monitoring and responding to changes in how their partners and customers do business, the more effective they will be in recognising and meeting regulatory expectations.

Sengupta: FIs and other financial intermediaries are at increased risk due to the growing regulatory obligations being enforced across global financial centres. Reliance on market-leading technology, or RegTech, in the AML space has become crucial, to monitor negative news, identify enforcement actions against customers and third parties, identify politically exposed persons (PEPs), identify suspicious transactions, and obtain beneficial ownership information. Failure to

adequately manage money laundering risks can bring significant reputational harm and expensive internal investigations, as well as the potential imposition of monitors or independent consultants to oversee remediation programmes, which can be disruptive and costly to the business. While FIs are the most exposed as the most commonly used intermediaries in cross-border money laundering activities, new categories of actors are starting to come under the purview of regulators, such as art market intermediaries, including auction houses, galleries, dealers, freeports, and so on, as well as crypto asset platforms.

Begum: The regulators appear to be taking a more assertive role when it comes to countering financial crime, which results in heightened pressure on firms to strengthen their AML systems and controls. A robust due diligence and KYC system remains key to a successful and transparent business relationship. This translates into having a clear and bespoke risk-based approach for firms to understand the risks they are exposed to, and what the best mitigation measures are. Economies are constantly evolving and new ways of doing business are being developed which requires firms to be proactive in terms of keeping their due diligence measures and risk approach regularly updated to meet their regulatory obligations and to keep their business protected from being used to carry out illicit activities.

Russo: Recent money laundering scandals such as the FinCEN files have shown how certain companies still suffer from deficiencies in setting up proper AML control mechanisms. This type of negative media attention affects a company's reputation, which in turn generates adverse financial repercussions. For example, when the FinCEN files were published, the main banks involved recorded historic drops in their stock value on financial markets. This attests to the fact that companies that do not comply with their obligations by not effectively combatting money laundering are creating a loss of financial value. Companies' – especially banks' – public exposure for lack of proper AML compliance methods generates a counterreaction from policymakers who provide for stricter rules. Consequently, AML supervisory authorities that apply those rules tend to impose heavier sanctions on non-compliant entities. Given all these ex-post risks and costs, companies are encouraged to be proactive about employing optimal KYC and due diligence methods and developing new tools to avoid ex-post backlash. On the upside, by complying with high KYC and due diligence standards, companies are also applying other compliance requirements such as anti-corruption third party due diligence. It is a virtuous circle. Against the development of increasingly sophisticated methods available to launder dirty money, notably through the development of e-finance, banks obviously have a crucial role to play as gatekeepers. They must therefore adapt by developing new monitoring tools that will enable them to carry out this task as effectively as possible, while the regulatory environment is increasingly strict and pressure from public opinion on this subject escalates.

FW: How should companies go about assessing whether their current AML measures are adequate in the current landscape?

Begum: In assessing whether a firm's AML measures are adequate, there are two main elements to consider: the risk appetite statement (RAS) and broader 'business-wide' risk assessment (BWRA). This is supported by the fact that firms can determine the types of risks that could adversely impact their business and the measures in place to mitigate these. On completion of the BWRA, where both external and internal financial crime threats have been considered, it should be incorporated into the firm's RAS. This assessment will then impact the firm's systems and controls, policies and procedures, training and reporting. A comprehensive analysis of the outcomes will enable firms to decide how best to adjust their AML measures to tackle those risks.

> "FIRMS NEED TO UNDERSTAND WHERE THEIR RISKS LIE, WHAT THOSE RISKS ENTAIL FOR THEIR OBJECTIVES, AND WHAT MEASURES THEY SHOULD BE TAKING TO MITIGATE THEM."
>
> NABEELAH BEGUM
> Norton Rose Fulbright LLP

Russo: The AML legal and regulatory landscape is ever more complex and evolving. In addition, practical indications on appropriate AML measures are not usually found in the law or in regulations themselves. Regulatory authorities, whether they are on a national or supranational level, as well as the FATF have published soft law guidelines containing concrete and technical

indications of which AML methods they consider adequate. Creating a specific function in a company to centralise information and constantly be updated on different worldwide standards, so as to establish a regulatory map to apply the highest compliance standards around the globe, is therefore an essential first step. Companies can also take initiative by innovating their AML tools without having to wait for specific guidelines. Indeed, faster, more automatised technical means of detecting suspicious activities, using artificial intelligence (AI) and oriented toward closing the gaps in the existing AML framework, are bound to be considered adequate, especially if the solutions found are ahead of current market practices.

> WHILE FIS ARE THE MOST EXPOSED AS THE MOST COMMONLY USED INTERMEDIARIES IN CROSS-BORDER MONEY LAUNDERING ACTIVITIES, NEW CATEGORIES OF ACTORS ARE STARTING TO COME UNDER THE PURVIEW OF REGULATORS.
>
> JOYDEEP SENGUPTA
> Mayer Brown

Sengupta: Regulated entities should seek periodic legal advice to ensure their current AML measures are consistent with applicable regulatory obligations in every jurisdiction in which they operate. For FIs, it is important to benchmark against industry practice to ensure the level of risk being accepted is not inconsistent with their similarly situated peers. Periodic risk assessments should be performed to identify potential gaps in the entity's controls, supplemented by periodic testing of such controls by internal and external auditors. Considering evolving developments, such as the situation in Russia, additional compliance resources may need to be directed to address high-risk areas, depending on the type of exposure facing the company. Finally, national regulator guidance is crucial in addition to international standards issued by intergovernmental bodies.

Fisch: Companies should, first and foremost, use periodic AML-specific risk assessments to assess their AML risk profiles. Risk assessments should evaluate the risk posed by the company's products and services, customers and geographic locations, among other risk factors, as well as the adequacy of a company's existing controls to address such risk. The risk assessment should consider changes in the technologies deployed by or available to the company. While new technologies, such as cryptocurrencies, may give rise to novel AML risks, they may also present opportunities to mitigate AML risk; for instance, by allowing companies to better analyse customer or transaction data to identify red flags. Periodic independent audits of the company's AML programme are another important tool in assessing whether the company's controls are adequate to address ongoing AML risks. Depending on a company's regulatory status, periodic risk assessments and independent audits may be required by law. Even in the absence of a specific legal requirement, they are often undertaken as a method of risk mitigation and an industry best practice. Once a risk assessment is conducted, companies should be prepared to make timely changes in response to the findings and remain nimble in the face of an ever-changing technological and regulatory environment.

Dawar: There is a very defined framework for credit institutions and all professionals in the financial sector in Luxembourg, for example circulars CSSF 11/519 and 11/529 on the risk analysis regarding the fight against money laundering and terrorist financing and circular CSSF 21/782 on money laundering and terrorist financing risk factors. These help firms to build a risk assessment which should serve as the basis for building an AML framework but also for measuring the effectiveness of the AML measures that have already been put in place. The 'National Risk Assessment of ML/TF' – which came into force on 15 September 2020 – has also provided Luxembourg entities with an understanding of the methodology to be applied and has been supplemented by additional sub-sector risk analysis. The business-wide money laundering and terrorist financing risk assessment that a professional has to perform should contain certain criteria as a minimum, which include its business activity and nature of its services, its investors on the liability side, its delivery channels, its investments on the asset side, its delegates and the countries or geographical areas it is exposed to in the liability and asset sides. Also, it is very important for firms to understand that competent authorities expect not only a qualitative but also a quantitative analysis, so firms must put in place key performance indicators (KPIs) to constantly monitor the evolution of their money laundering and terrorist financing risks and take measures accordingly. As part of their money laundering and terrorist financing risk assessment, firms should also factor in potential new emerging risks such as cyber crime, fraud, bribery and corruption, insider trading and market manipulation,

as communicated by competent authorities as part of their outreach programme through various conferences and industry forums.

FW: What benefits are new technologies – such as artificial intelligence and machine learning – bringing to AML processes? What steps can companies take to address typical challenges when integrating new solutions into their existing systems?

Russo: With the emergence of the digitalisation of financial transactions, one of the most important difficulties in implementing effective AML control is analysing large amounts of cross-border transaction schemes that are made in short periods of time. The first benefit of AI and machine learning (ML) to KYC processes is that they are instrumental in solving this issue, especially by improving the quality, completeness and consistency of client data. Moreover, they are advantageous compared to manual KYC methods because they are able to run perpetually and may represent, on average, up to a 20 percent reduction of company costs. Finally, these technical tools that find inconsistencies in the analysed data, at the right time, can save banks from heavy financial penalties for missing money laundering activities. Overall, intelligent automation (IA) and ML help companies increase their standards in complying with what is expected of them by regulatory authorities. This does not, however, exclude human decision making behind the data analysis provided by software.

Sengupta: Given the complexity of AML typologies, AI and related technology is essential to identifying efforts to hide money laundering. AML monitoring technology can now routinely identify typical suspicious transaction patterns, such as round numbers, no apparent business purpose, high frequency transactions involving the same parties, unexplained close in time inflows and outflows, multiple transactions just below a monetary threshold, involvement of multiple high-risk jurisdictions, and so on. We sometimes see new technology solutions being rolled in too quickly without sufficient testing in advance, which can lead to increased risks. Testing of new technology solutions by internal and external auditors is essential, which can help identify potential gaps in the monitoring technology, or incomplete application to capture all relevant fields in payment messages. Guidance from local regulators is also helpful to ensure expectations are aligned.

Fisch: New technologies play an increasingly pivotal role in AML compliance, particularly for businesses with exposure to virtual assets. There are many new, sophisticated tools that analyse information available across various blockchains to help identify transactions and wallets that may be engaged in suspicious or potentially unlawful activity. This type of blockchain analysis is becoming increasingly common. New technology may also help FIs automate various reporting, record keeping and information sharing processes required under applicable AML rules. These new compliance tools evolve almost as rapidly as the activities they are frequently designed to monitor. This presents challenges with the implementation and integration of new technology into a company's established back-office and compliance infrastructure. It is therefore critical that companies devote sufficient resources to the rollout and continued testing of new compliance technology. One frequently recurring problem seems to be that companies underestimate the time and work needed to successfully integrate and operationalise new technology, which may, in turn, create unexpected gaps in their compliance programme or exacerbate related compliance risk.

Dawar: Current approaches to fighting money laundering and terrorist financing are labour intensive and time consuming, which therefore makes them expensive. AI and ML allow firms to scan enormous amounts of data, to identify behaviours, patterns and anomalies faster than any humans can, such as PEP and sanctions screening, as well as transaction monitoring processes, for instance by reducing the number of false positive alerts. This allows firms to better prioritise their resources on a risk-sensitive basis and address higher risk situations with the benefit of human experience and expertise, to fight financial crime more effectively. The two biggest challenges in implementing new solutions such as AI and ML are data quality and tackling bias in AI. Therefore, it is important for firms

> "REGULATORY PRESSURE ON FIRMS IS HIGH AND THE SHEER NUMBER OF REGULATIONS THAT HAVE BEEN PASSED OVER THE PAST FOUR YEARS IS TESTIMONY TO THIS."
>
> ABHISHEK DAWAR
> Arendt Regulatory and Consulting (ARC)

to understand that AI is a journey and not a 'plug and play' exercise. Moreover, prior to integrating AI solutions, it is imperative that firms carry out an AI maturity assessment, which starts by understanding 'test cases' within AML processes where implementing AI can help.

Begum: AI and ML are two major technological advances. An advantage of these is associated with how these new developments may allow firms to better learn patterns in transaction monitoring, which would enable firms to make use of technology to apply relevant detection techniques based on an identified pattern of activity that is determined in conjunction with the firm's existing systems. This integration will usually be beneficial to quickly identify and mitigate unwanted risks. There is also the possibility that these technologies can create gaps in firms' policies and procedures that may remain unnoticed for some time, and, in some cases, unintentionally allow illicit activities to take place. It is imperative that firms frequently update their systems and keep track of changes and implement new measures to tackle any potential risks that may come with new technological advancements.

FW: What essential advice would you offer to companies seeking to create a robust AML programme that ensures ongoing compliance with the evolving regulatory landscape? What are the main issues and challenges that need to be overcome?

Begum: The key to a robust AML programme is having a well-developed and regularly updated risk assessment system. Firms need to understand where their risks lie, what those risks entail for their objectives, and what measures they should be taking to mitigate them. Firms can then use this to implement proportionate controls. This should be a dynamic approach; as the regulatory landscape evolves, there needs to be a reasonable action plan to identify and implement any changes that may be needed to control, and keep pace with, new risks that could potentially arise. These must be realistic measures assessed against realistic and specific scenarios for the particular activities of the firm. There is no 'one size fits all' approach – bespoke and comprehensive measures remain the best way forward in these instances.

Fisch: One key element for any successful AML compliance programme is performing a comprehensive assessment of the company's risks. A thorough understanding of the company's business model, its geographic footprint, and its customer and client base is essential. No two companies' risk profiles are exactly the same, and because regulators expect a risk-based approach to AML compliance, companies should tailor their AML compliance programme to fit their specific risks. Put differently, regulators expect companies to allocate finite AML compliance resources logically and efficiently. It is crucial that a company be able to explain to regulators why its compliance programme is structured and focused in a certain way, particularly if any compliance issues were to arise. A company's risk profile may also change over time. For example, a company that adopts or deals with new technology – such as distributed ledger technology and virtual assets – may be faced with materially different risk parameters. It is, therefore, important to conduct risk assessments on a regular basis and immediately take steps to counter any newly identified risk, including through the deployment of new AML compliance technology where appropriate.

Dawar: Understanding the money laundering and terrorist financing risks faced by businesses is the first step in creating a robust AML compliance programme; therefore, articulating the inherent risk a firm is willing to undertake as part of its AML risk appetite statement is of utmost importance. An AML risk appetite should be the cornerstone of an AML risk-based approach and the design of mitigating controls should include policies, procedures and processes. Furthermore, dedicated specific training programmes for employees to be able to detect, prevent and report money laundering and terrorist financing will help firms make their AML programmes not only compliant with an evolving regulatory landscape, but also increase their effectiveness in the fight against money laundering and terrorist financing. When it comes to the main issues, keeping an AML programme up to date with a fast evolving legal and regulatory framework remains the biggest challenge for firms. In order to address this, firms should embrace a culture of self-evaluating AML and CTF mitigation controls as part of an annual, company-wide money laundering and terrorist financing risk assessment to ensure that these controls are effective in mitigating business risks.

Sengupta: A robust AML programme must be periodically adapted to address emerging risks, such as the COVID-19 pandemic, the Russian invasion of Ukraine, supply chain disruptions, and so on. One size does not fit all, so the risks for a large FI would be very different from a small private bank or a FinTech firm. The standard elements of a robust programme will include tailored policies and procedures, internal controls that effectively monitor risks, including customer and third party due diligence, periodic training, and internal and external audits. FIs should seek periodic legal advice to ensure compliance with evolving standards across the jurisdictions where they operate. A compliance culture with open lines of communication, including secure whistleblowing channels, is also important. A strong tone at the top is necessary to promote a culture of AML compliance, as well as an independent compliance team that is capable of escalating issues in a timely manner so they can be remediated or reported, consistent with legal obligations.

Russo: Today, despite progress made in AML programmes and incremental legal and regulatory oversight, certain practical issues remain in how compliance is implemented. One of the main issues is the capacity for companies to adapt their AML control processes not only to a rapidly

evolving regulatory landscape, but also to emerging and ever-changing practices developed by criminals to circumvent regulation or company compliance programmes. Given the advanced technologies that are used, one of the main elements companies will have to focus on is their adaptability in order to keep up. Automation in AML processes such as screening alert remediation and transaction tracking is crucial, but its capacity to be easily and swiftly modified in reaction to changes in practices and regulations will be vital for economic actors. Lastly, in some compliance fields, companies can also increase collaborations with RegTech companies so issues can be flagged before they worsen, allowing for a higher level of proactivity.

FW: What are your predictions for AML trends through 2022 and beyond? How are regulations likely to evolve?

Fisch: Against the backdrop of rapid technological change, US and other regulators have stressed a technology-neutral approach to AML regulations. Regulators tend to believe that similar financial products and services should be subject to the same kinds of AML requirements, regardless of the technologies that underpin them. We expect regulators to continue to focus on blockchain technologies and virtual assets. While US and other regulators have weighed in on the regulatory treatment of certain types of players in this space, there are still open questions about the treatment of certain products and services. Governments have also expressed considerable interest in stablecoins and central bank digital currencies (CBDCs), and the Biden administration is exploring the risks and benefits related to those technologies. Given the complexity of the policy issues surrounding stablecoins and CBDCs, we do not expect to see new legislation until late 2022 or early 2023 at the earliest. We also expect enforcement agencies will continue to bring civil and criminal enforcement actions against companies and individuals that fail to comply with AML laws and regulations, with particular focus on the digital asset space.

Dawar: AML will definitely remain a hot topic for the market over the next few years. The enhancement of cryptocurrencies and virtual asset regulations, emerging technologies such as AI and ML, data sharing among non-group related FIs to combat money laundering and terrorist financing, expanding AML and CTF laws and regulations beyond financial professions, and changes to beneficial ownership requirements, will all shape AML trends through 2022 and beyond. Furthermore, in July 2021, the EC presented an ambitious package of legislative proposals aimed at strengthening the EU AML framework. This initiative followed a number of alleged money laundering cases which highlighted the fragmented state of AML architecture at an EU level, including divergences between national regimes and a lack of cooperation between AML authorities. To address these issues, the EC proposed the establishment of a new EU AML authority to supervise institutions that pose the highest risks and to promote a higher degree of cooperation between AML authorities. The EC also proposed the adoption of a new EU regulation that would be directly applicable to all EU member states. Going forward, although the key pillars of AML rules will remain, their content will overall be strengthened. At an EU level, the focus will be on continuing to improve convergence, cooperation and supervision, which will also lead to greater convergence and standardisation of market practices in relation to customer and ongoing due diligence processes.

Sengupta: Following recent developments in Ukraine, we have seen unprecedented cooperation between major economies, including the EU, US, UK, Switzerland, Japan and others, on the sanctions front. Given the frequent overlap between economic sanctions, anti-corruption and AML enforcement efforts, we are likely to see continued international cooperation, including regulatory convergence and joint enforcement actions, as recently demonstrated by the creation of an EU AML authority. FIs are likely to face increased costs and monitoring obligations relating to transactions involving high-risk countries, alternative assets and private banking activities, including more stringent reporting obligations. Industries closely tied to the private banking world, including art, alternative investments, private equity, luxury real estate, jewellery, watches and so on, are likely to face increased regulatory scrutiny and reporting requirements, in addition to the new technologies already being targeted by the authorities, such as cryptocurrencies and digital assets.

Russo: Recent money laundering cases have shown that there is a greater need for transparency and recent legislative and regulatory efforts have reflected the desire to reach this objective. Furthermore, the fact that they are implemented in reaction to current phenomena shows the need to anticipate emerging, very sophisticated money laundering practices and resolve ongoing issues that still exist in AML processes. Therefore, ultimate beneficial owner (UBO) regulation and increased guidelines on technical means allowing for better traceability of funds and crypto assets are likely to emerge. Governments, regulatory authorities and international organisations are likely to increase their coordination to launch better regulatory requirements and frameworks but also to better coordinate their enforcement actions. Finally, regulation scopes will continue to extend beyond FIs. For instance, the FATF determined in a May 2022 evaluation report that France has a robust and sophisticated framework to fight money laundering and terrorist financing that is effective in many respects but recommended better supervision of certain fields that are increasingly exposed to financial crime, such as real estate.

Begum: There are many areas and trends in terms of AML going forward. With respect to the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (MLRs), the proposed amendments to the rules, taking into

account HM Revenue & Customs' consultation in 2021, are due to take place in 2022. The amendments will mainly address the scope of the MLRs, how SARs can be accessed and viewed once submitted, clarity on the definition of a credit or a financial institution, how information is shared and gathered for intelligence purposes, and the ability to give the FCA additional supervisory powers with respect to Annex I MLR registered firms. In terms of sanctions, given the current conflict in Ukraine, the FCA has published a new webpage concerning its expectations of firms considering the UK's sanctions on Russia. The key message from the FCA is that it expects firms to have established systems and controls to counter the risk that they might be used to further financial crime, and this includes compliance with financial sanctions obligations. Firms continue to face scrutiny regarding the extent to which they have addressed AML risks effectively and this issue is expected to remain a key area of enforcement focus for the FCA throughout 2022. Last year, the FCA brought its first successful criminal prosecution under the MLRs. One of the lessons learned from the published cases is not only undertaking periodic reviews to check that procedures are clear, but also ensuring that there is evidence that they have been understood, followed and are achieving the desired outcomes. ■