REPRINT

R&C risk & compliance

DEVELOPMENTS IN EUROPEAN ANTI-MONEY LAUNDERING

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2022 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

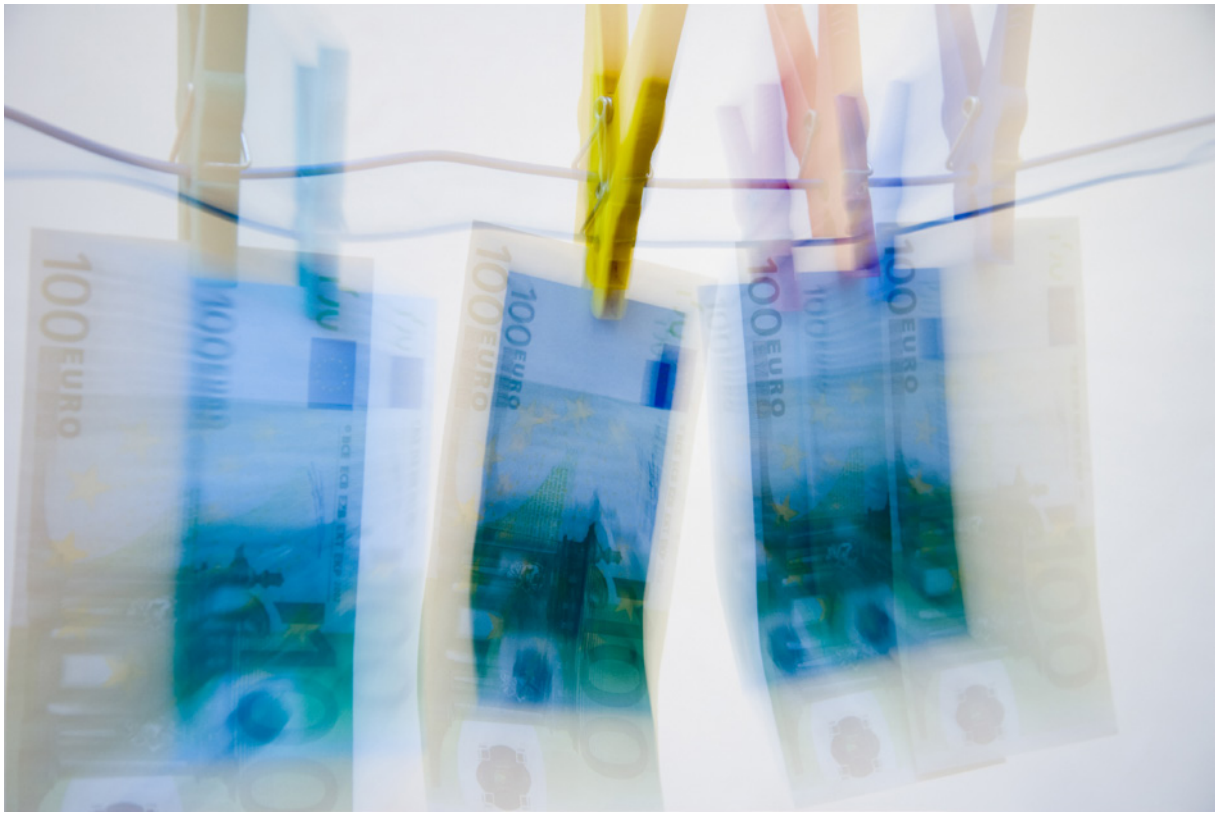
PESTALOZZI
ATTORNEYS AT LAW

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

HOT TOPIC

DEVELOPMENTS IN EUROPEAN ANTI-MONEY LAUNDERING



PANEL EXPERTS

Joydeep Sengupta
Counsel
Mayer Brown
T: +33 (1) 5353 3949
E: jsengupta@mayerbrown.com

Joydeep Sengupta is a member of the compliance, investigations and regulatory team at 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 anti-corruption laws.

Hannah Meakin
Partner
Norton Rose Fulbright LLP
T: +44 (0)20 7444 2102
E: hannah.meakin@nortonrosefulbright.com

Hannah Meakin is a financial services regulation lawyer based in London. Her practice focuses on market infrastructure, commodities derivatives and FinTech. She advises on all aspects of compliance with relevant PRA and FCA requirements and has particular knowledge of brokerage, exchange trading, clearing, settlement, custody, client money and wholesale conduct. She helps clients understand and implement financial services legislation, including MiFID II, MAR, EMIR and the CRR, and has led client projects on each of these.

Andrea Huber
Partner
Pestalozzi
T: +41 (44) 217 9241
E: andrea.huber@pestalozzilaw.com

Andrea Huber is a partner and member of Pestalozzi's financial services group specialising in banking and regulatory matters including FinSA and FinIA, asset management and investment funds, FinTech, capital market transactions, compliance and white-collar crime. She regularly represents clients in proceedings before the Swiss Financial Market Supervisory Authority (FINMA), the SIX Swiss Exchange and the CDB Supervisory Board (VSB Aufsichtskommission).

Eric Russo
Partner
Quinn Emanuel Urquhart & Sullivan LLP
T: +33 (1) 7431 3520
E: ericrusso@quinnemanuel.com

Eric Russo is a partner at Quinn Emanuel Urquhart & Sullivan LLP. His practice focuses on white-collar crime, regulatory investigations, compliance and litigation. He advises and assists global corporations and their managers in the conduct of internal investigations and in the context of enforcement proceedings, in Europe and in the US. His expertise also covers financial market abuses and corporate and commercial litigation. Formerly a public prosecutor, Mr Russo carried out several landmark criminal investigations related to money laundering and international corruption.

R&C: Could you provide a general overview of money laundering activity in Europe? What trends have you observed in recent years?

Meakin: Illicit activity continues to be a prevalent issue. Over the last few years, money laundering has increased and, according to Europol, around 1 percent of the European Union's (EU's) annual gross domestic product is "detected as being involved in suspect financial activity". This is due to the expanding nature of predicate offences moving from traditional nefarious activity of crime and drug-related offences to more niche and intricate methods which technological advancement has nurtured. There is an increased risk presented by the surge in popularity of virtual currencies that allow for increased anonymity. Moreover, most recently, the change in behaviours due to the coronavirus (COVID-19) pandemic has led to new money laundering activity.

Huber: Anti-money laundering (AML) is and remains a highly critical issue in Switzerland as a leading global cross-border wealth management hub for private clients. A look at the latest annual report from the Swiss Financial Market Supervisory Authority (FINMA) shows that the Anti-Money Laundering Act (AMLA) is not only one of the focus points of conduct supervision by FINMA but also plays a central role in enforcement. The recently published 'FINMA Risk Monitor' also highlights the fact that Switzerland is particularly exposed to money laundering risk. New customers of the Swiss asset management industry are often found in emerging markets where there is a significant risk of corruption. Experience shows that, in addition to wealthy private clients who often qualify as politically exposed persons (PEPs), state-owned or state-related enterprises and sovereign wealth funds are also involved in financial flows associated with corruption and embezzlement. The risks are increased further by complex structures that can cloud transparency on the beneficial ownership of assets concerned. These structures include domiciliary companies, fiduciary relationships and insurance wrappers.

Russo: It is possible to observe that money laundering in recent years combines older methods with newer ones that have been developing through time. Recent money laundering trends are related to the increasing importance of digital services. Indeed, it is reported that money launderers now increasingly rely on the virtual assets sector, meaning their methods increasingly include the use of cryptocurrencies, and other components of the rapidly evolving ecosystem of decentralised finance. This alternative system removes the traditional forms of control that banks and institutions have on financial flows and services because of reduced traceability. The more limited regulation of

decentralised finance compared to the traditional banking sector is also a facilitating factor.

Sengupta: Europe has seen a tremendous regulatory and enforcement focus on money laundering in recent years, with multiple domestic and cross-border investigations bringing to light increasingly complex typologies of money laundering. They often involve multicurrency fund flows over long periods involving offshore jurisdictions, obscure shell companies and complex transactions involving unusual asset classes. High-profile financial scandals, such as the Panama Papers, Pandora Papers, Paradise Papers, the Russian Laundromat and Swissleaks, have touched nearly every major financial centre in Europe, including the private banking sector. Decades of financial scandals and terrorist attacks have led EU countries to adopt an AML-countering the financing of terrorism (CFT) framework that includes, among other things, EU AML Directives, as well as the recommendations of the Financial Action Task Force (FATF). Actors such as Moneyval, the Council of Europe body assessing compliance with AML/CFT, and the Egmont Group, the international platform for secure exchange of expertise and financial intelligence between financial intelligence units (FIUs) for AML/CFT, have also had a significant impact on the European prevention and enforcement landscape in recent years.

R&C: To what extent has the coronavirus (COVID-19) pandemic increased the opportunities for money laundering, particularly with the mass shift to remote working?

Huber: Reports to Switzerland's Money Laundering Reporting Office (MROS) rose 25 percent in 2020, with many of them related to COVID-19 credits. MROS received 5334 such reports in 2020, concerning more than 9000 business relationships. Nearly 90 percent of these reports came from banks. They included 1046 reports relating to COVID-19 credits granted by financial institutions (FIs) under the guarantee of the Swiss federal government. They concerned 1054 loans granted by 43 different banks, totalling approximately CHF149.6m. MROS further warned that the pandemic has provided criminals with new opportunities for illegal enrichment, thus increasing the risk of money laundering. While new technologies facilitate efficiency improvements in financial services, the threats of money laundering and the financing of terrorism are also heightened due to the potential for greater anonymity along with the speed and cross-border nature of transactions.

Russo: The COVID-19 pandemic has indeed pushed individuals and companies into remote working and increased online activity. This, in turn, has fostered an emergence of cyber crime, including email and SMS phishing attacks, ransomware

and business email compromise scams. FATF has highlighted that such illicit behaviours have created new sources of proceeds for illicit actors. The layering of illicit revenue has also benefitted from the increase in remote transactions through misuse of the formal banking system, the decentralised banking sector and investment in cryptocurrencies.

Sengupta: Stay at home orders and remote working have shifted dependence on technology to new heights, fostering an increased reliance on the digital world. Opportunities for money laundering arise from hidden information regarding the ultimate beneficial owners, the origin or final destination of funds. Remote working also reduces the opportunity for in-person contact with clients and site visits with intermediaries, which may make it easier to conceal or disguise certain types of information, and is detrimental to proper third party due diligence and know your customer (KYC) checks. FATF produced a helpful report in May 2020 detailing COVID-19-related money laundering and terrorist financing risks and policy responses. This report lists increased fraud, including impersonation of officials, counterfeiting, fundraising for fake charities and fraudulent investment scams, cyber crime, business email compromise scams and ransomware attacks, which have contributed to greater money laundering activities.

Meakin: The COVID-19 pandemic has led to an increase in opportunities for individuals involved in money laundering. There was a vast change in customer attitude and behaviours and, as a result, the way in which customers utilise the financial system. During this period there was significant uptake in digital services. Money launderers were able to evolve their techniques, leading to a well-publicised rise in fraud, with vulnerable individuals often being the target. In relation to the mass shift to remote working, it placed more pressure on the system to detect and stop money laundering, in real-time.

> **"In view of constant technological changes, corporations can no longer rely on manual KYC processes to get by in their AML efforts."**
>
> *Eric Russo,*
> *Quinn Emanuel Urquhart & Sullivan LLP*

R&C: What legal and regulatory developments have been aimed at tackling money laundering across Europe? To what extent have authorities increased

their anti-money laundering (AML) monitoring and enforcement efforts?

Russo: On 21 June 2021, the European Commission (EC) released an elaborate package of legislative proposals to strengthen the EU's AML and CFT rules, as a way to close loopholes money launderers may use. This package includes the establishing of a new EU AML/CFT authority, a new EU regulation on AML/CFT containing directly-applicable rules in EU member states, and a revision of Regulation 2015/847/EU on Transfers of Funds to trace transfers of crypto assets. It constitutes adapting the regulation toward newer methods of fraud observed during the pandemic by closing gaps that may exist in the financial system and focusing on increased coordination between EU member states, such as increased information sharing and means of action.

Meakin: There have been significant developments in the legal and regulatory system within the EU. In July 2021, the EC published a package of legislative proposals aimed at strengthening the EU's AML and CFT rules. The package consists of four legislative proposals. First, a regulation establishing a new EU AML/CFT authority. Second, a regulation on AML/CFT, containing directly-applicable rules, including in the areas of customer due diligence (CDD) and beneficial ownership. Third, a sixth directive on AML/CFT (AMLD), replacing the existing Directive 2015/849/EU, the fourth AML directive as amended by the fifth AML directive. Finally, a revision of the 2015 regulation on transfers of funds to trace transfers of crypto assets. In addition, in December 2021, the European Banking Authority (EBA) decided to strengthen its AML/CFT supervision by issuing its revised guidelines on risk-based supervision of credit and FIs' compliance with AML/CFT requirements.

> **"The increase in the number of MROS reports indicates a cultural shift as well as better monitoring systems, but also the continued existence of a number of significant risks."**
>
> *Andrea Huber, Pestalozzi*

Sengupta: One of the most significant recent European AML developments was the AML and CFT legislative package in 2021, which contains four legislative texts aiming at harmonising AML laws across member states. Firstly, the EC has put

forward a draft proposal for an AML regulation, which will give more detail into CDD requirements and adapting third country policy. Secondly, the 6AMLD provides details on the beneficial ownership register and strengthens cooperation between FIUs. Thirdly, there are proposed amendments to an EU regulation to facilitate the tracing of transfers of crypto assets. Finally, and perhaps most importantly, a regulation establishing the authority for AMLA has been proposed, to ensure more harmonised monitoring and enforcement. This European body will monitor developments across member states and third countries, establish a central database compiling information from supervisory authorities, and analyse the information collected to support, facilitate and strengthen cooperation and exchange of information. In terms of enforcement, it is also tasked with ensuring group-wide compliance carrying out supervisory reviews and assessments.

Huber: FINMA has been dealing with five enforcement cases in 2020 in connection with Venezuelan oil conglomerate PDVSA. These cases clearly illustrate that a bank's compliance framework must be adapted in line with risk appetite, institutions must establish the provenance of assets and whether the clients concerned are indeed the beneficial owners, and they must report any dubious relationships to MROS. The increase in the number of MROS reports indicates a cultural shift as well as better monitoring systems, but also the continued existence of a number of significant risks.

R&C: What solutions are being deployed by companies in Europe to tackle money laundering? To what extent is technology being used to enhance processes, warnings systems and controls?

Sengupta: The European AML landscape is diverse and FIs must keep pace with developing rules and regulations in order to meet their compliance obligations, as enforcement actions are on the rise. Supervisory authorities have the power to impose a set of sanctions that are effective, proportionate and dissuasive, so it is essential that the applicable AML regulations are properly applied. FIs must meet more and more obligations to fight money laundering and terrorist financing, and prevent fraud. Innovative technologies, frequently dubbed 'RegTech', can automate some of these processes and simplify the management of risks related to regulatory non-compliance. The EBA wants to boost the adoption of these solutions by harmonising rules within the EU and improving market knowledge. KPMG identified more than 240 startups in Europe, including about 50 in France, in its overview of the RegTech ecosystem, and AML is the most represented segment.

Huber: Money laundering is a serious problem for the global economy. Customer risk-rating models are one of the primary tools used by FIs to detect money laundering. The models deployed by most institutions nowadays are based on an assessment of risk factors, including the customer's profession, salary and the banking products used. Such information is collected when an account is opened, but it is infrequently updated. Based on the law as currently in force in Switzerland, the contracting party only has to be identified again if doubts arise in the course of the business relationship regarding the information on the identity of the contracting party or the beneficial owner. FATF qualified the lack of an explicit obligation to ensure that customer data is up to date as a significant deficiency in its 2016 country report. Under the revised AMLA, a regular review of all business relationships, in particular with regard to KYC, is therefore required.

Meakin: The advancement in technology, while leading to new and innovative ways for nefarious actors to money launder, has also equally posed significant opportunity for compliance and the fight against money laundering. Many software providers are available that aim to protect companies from financial crime and make it easier to detect finance crime. This software includes sanction screening, politically exposed person screening, automated identification and verification services, and automated transaction-monitoring software.

Most technological solutions can be calibrated and tailored, which further enhances the ability to tackle money laundering.

Russo: In view of constant technological changes, corporations can no longer rely on manual KYC processes to get by in their AML efforts. Instead, they need to adopt more advanced solutions that can spot suspicious behaviour in online account activity using multitiered identity management tools that can quickly report or block any suspicious activity. The pandemic and remote work have accelerated advances in areas such as identity verification. The focus through this shift has been improving data quality and using data analytics, machine learning and automated processes, such as screening, alert remediation and transaction tracking – motivated in part by the emerging requirement for perpetual KYC. In addition, organisations will need to continuously monitor customers after onboarding to detect any changes in status that may increase their risk level. Finally, because of increasing levels of crypto crime, the more sophisticated countermeasure now appears to be the development and deployment of blockchain KYC solutions.

R&C: Do you believe companies need to enhance the due diligence and background checks they carry out on their business partners and customers?

Huber: As of 1 July 2022, Swiss financial intermediaries must verify the identity of beneficial owners and periodically review and update client files instead of merely identifying them, as was the case up to now. Pursuant to the new law, the financial intermediary must exercise due diligence required under the circumstances to establish and verify the identity of the beneficial owners. Based on the government dispatch, the financial intermediary may take a risk-based approach and, therefore, apply different measures to ensure the plausibility of the beneficial owner's information. The required form and depth of the review, however, is unclear under the new statutory amendments.

Meakin: CDD is the foundation of the KYC principle. The KYC principle is a requirement for companies to ensure that they understand who their customers are, their financial behaviour and the extent of the money laundering risk they present by doing business with them. As such, CDD remains one of the most important ways to combat money laundering. Companies are required to adopt a risk-based approach to compliance, and with this apply enhanced CDD measures where required. Companies should continue to remain vigilant and use their risk appetite, their understanding of a customer and their activities to guide the extent of CDD measures conducted.

Russo: In the EU, each member state has an AML supervisory authority which is responsible for monitoring the national AML/CFT regime and verifying compliance by reporting entities. Such authorities can impose fines for non-compliance or even report the case to another regulator. The US and the UK generally follow an equally punitive regime in the application of money laundering rules and sanctions. In recent years, significant fines and other sanctions have been imposed on EU banks operating abroad. It is important that companies, and especially banks, enhance the due diligence and background checks they carry out to avoid sanctions. Moreover, French legislators have introduced strict obligations in terms of third party due diligence for both anti-corruption and AML. Disregarding appropriate diligence and checks can also lead to sanctions by regulatory authorities. Given the risk incurred in terms of sanctions, companies are encouraged to further enhance third party due diligence and to continue to develop new tools.

Sengupta: For many companies operating in high-risk sectors of the economy, or with multiple touchpoints with high-risk jurisdictions, it is advisable to enhance their due diligence policies and background checks based on the level of risk and using a defensible methodology. The EU perceives due diligence as an essential element in combatting money laundering. However, while historically

due diligence was only applied to customers, it is becoming increasingly common with other stakeholders, such as partners, consultants and suppliers. It may also be necessary to renew due diligence and background checks periodically, and especially in light of any negative news or material change in the entity. The EU AMLDs provide different levels of customer due diligence: simplified, normal and enhanced measures. Enhanced due diligence measures must be put in place when a product or transaction presents a high risk of money laundering and terrorism financing and for any particularly complex transaction of an unusually high amount that does not appear to have any economic justification of lawful purpose.

entity or the type of transaction in question. Thus, a private bank establishing a new foreign client relationship with the purpose of performing high-value commercial transactions using a complex structure would need to apply higher standards than a routine relationship with a domestic client operating domestically in a low-risk sector of the economy. Large EU countries may have more restrictive obligations than other countries which may be difficult to implement, but compliance is essential to effectively fight money laundering and terrorist financing. Because enforcement actions vary significantly from jurisdiction to jurisdiction, legal advice should be sought as to whether a declaration should be made.

"Companies should continue to remain vigilant and use their risk appetite, their understanding of a customer and their activities to guide the extent of CDD measures conducted."

Hannah Meakin, Norton Rose Fulbright LLP

R&C: What advice would you offer to companies operating in Europe on establishing AML controls that can detect suspicious activities and serve as an effective red flag system?

Sengupta: Companies are required to comply with national laws and regulations applicable in the jurisdictions in which they operate. This includes following the obligation to detect and report suspicious transactions consistent with national laws and industry best practices. These obligations and control systems may vary based on the type of

Russo: Companies probably need to have a constant and sophisticated KYC approach and tools

due to how rapidly money laundering methods are evolving and how difficult it can be to have real-time data processing and analysis. The role of artificial intelligence (AI) must not to be neglected in this respect. AI can be very helpful to monitor and assess the multitude of cross-border transactions that take place over very short periods of time.

Meakin: Effective controls are a vital cog in the AML wheel. FIs need to continuously assess, review and, where needed, update their governance parameters on suspicious activities. AML can be a fast-moving environment and risks can change at a moment's notice. Ensuring FIs have the right mechanism to translate changes effectively through the business is critical – human determination is key. This becomes even more challenging with complex international organisations, so carefully managed information collaboration across the group is going to help. While technology is a key enabler for suspicious activity detection, it is important FIs have the right manual controls and oversight to support and ultimately report this. More generally, they need to ensure that routine training is carried out, and that the audience is as broad as needed.

Huber: We strongly recommend having a robust AML programme in place. This requires substantial investment because it calls for not only sufficient experienced resources, but also for advanced technology that can support the AML compliance function of the financial intermediary to better identify, measure, monitor, control and report on money laundering and the financing of terrorism risks. Failure to have an effective AML compliance programme can result in enforcement action from FINMA, including heightened regulatory scrutiny, costly remediation efforts and legal costs, as well as reputational damage. It further needs to be noted that cryptocurrencies are often used in connection with cyber attacks or as means of payment for illegal trading on the dark web. Money laundering risks can be significant for FinTech companies as well.

> **"The European financial centres that frequently serve as entry-points for proceeds of crime into the EU are expected to face heightened scrutiny."**
>
> *Joydeep Sengupta, Mayer Brown*

R&C: How do you envisage the fight against money laundering in Europe

developing in the months and years ahead? Are you optimistic about the prospects for improved systems that lead to a drop in financial crime?

Russo: The EU approach is very regulation-based. It seeks to implement common AML rules throughout the EU to combat cross-border money laundering more efficiently, especially in terms of increased information sharing. It is certain that in the future, stakeholders can expect first and foremost a more heavily regulated financial sector, in all its aspects. Moreover, KYC and AML compliance, in general, will be increasingly digitalised, as it allows for these processes to keep up to date with sophisticated methods used by cyber criminals and to respond better to legal and regulatory requirements. Finally, green crime is a new global threat that is likely to go hand in hand with money laundering. Green crime is very lucrative, posing risks to environmental and financial ecosystems by exploiting natural resources. This type of crime is growing significantly each year. Therefore, we can expect this concerning issue to be tackled by AML actors in the near future.

Meakin: With the recently proposed overhaul of the European legislative framework governing AML/CFT efforts, it is clear that the fight against financial crime remains and will continue to remain a priority for decision makers and enforcement authorities in Europe. More streamlined and directly applicable legal requirements, as well as a centralised supervisory framework, including the prospective introduction of a single EU AML authority, are expected to address the main shortcomings in AML/CFT enforcement in Europe – essentially, national fragmentation and the lack of a consistent approach to cross-border cooperation. This, coupled with continued technological developments allowing firms to deploy more advanced systems and procedures to comply with AML/CFT requirements, should result in an overall improvement in global efforts against financial crime.

Huber: The risks from complex and ever more sophisticated money laundering schemes will certainly increase in the future. Not only will detection systems improve, money launderers will also get more sophisticated. For instance, as banks and consumers push for the simplification and digitalisation of onboarding, new risks will arise. Therefore, financial intermediaries will need to improve their AML surveillance systems continuously in line with applicable laws and regulations. In line with the continued and increased regulatory regime, support for technology will be a prerequisite to enable financial intermediaries to further collaborate in building and improving their systems.

Sengupta: The fight against money laundering in Europe is expected to strengthen considerably,

especially in light of recent developments involving economic sanctions targeting financial transactions and assets relating to Russian oligarchs and Russian PEPs. The luxury real estate sector, investment-based 'golden visa' schemes, the art and cryptocurrency worlds are all expected to face increased AML scrutiny in light of sanctions against Russia. The creation of the new AMLA entity at the European level is expected to strengthen cooperation between different European jurisdictions, given the multijurisdictional footprint of most money laundering activity. The European financial centres that frequently serve as entry-points for proceeds of crime into the EU are expected to face heightened scrutiny. R&C