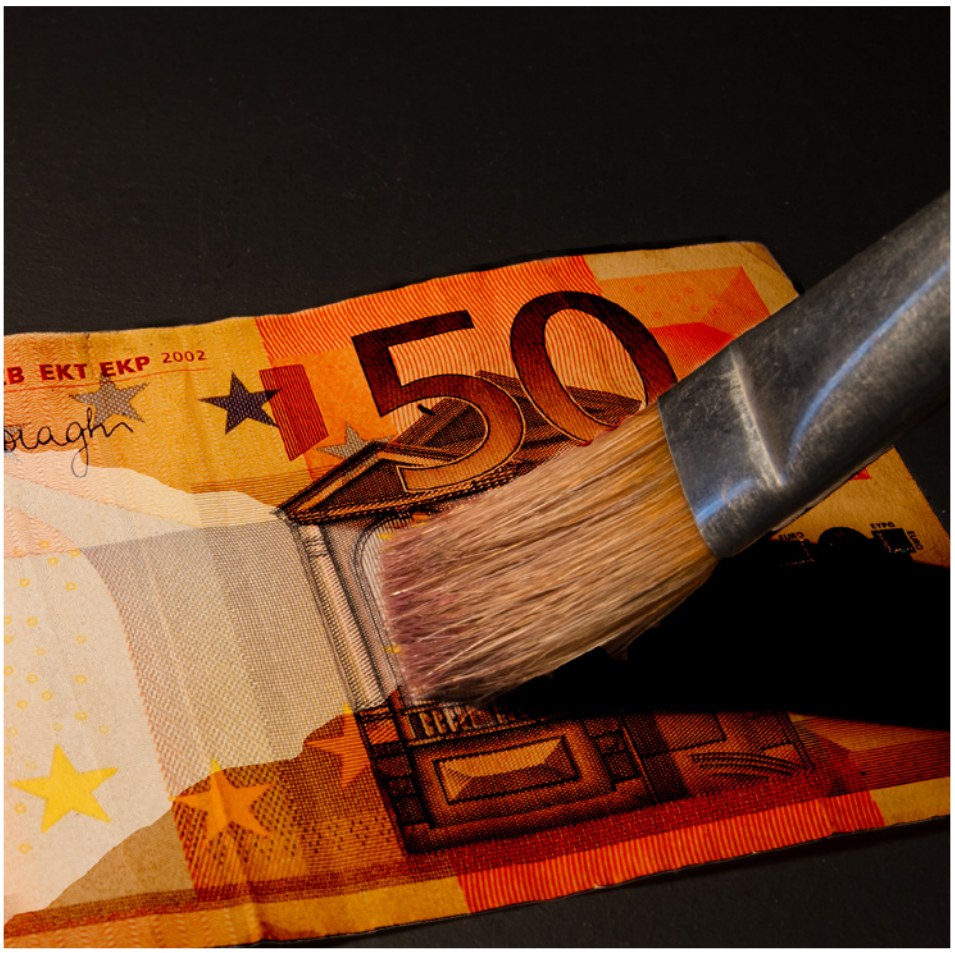
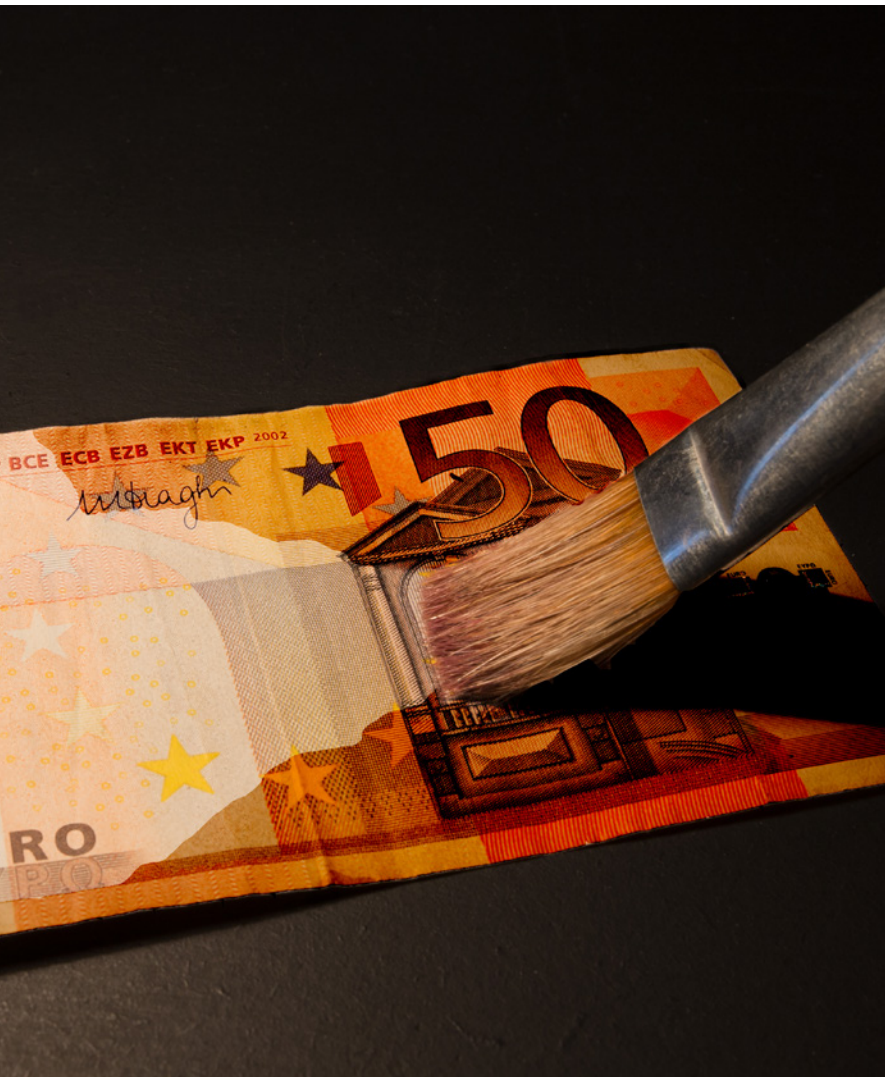


INDEPTHFEATURE

ANTI-MONEY LAUNDERING

2021

FINANCIER WORLDWIDE corporatefinanceintelligence



Published by
Financier Worldwide Ltd
First Floor, Building 3
Wall Island, Birmingham Road
Lichfield WS14 0QP
United Kingdom

Telephone: +44 (0)121 600 5910
Email: info@financierworldwide.com

www.financierworldwide.com

FINANCIER WORLDWIDE corporatefinanceintelligence

INDEPTHFEATURE

ANTI-MONEY LAUNDERING

February 2021

Introduction

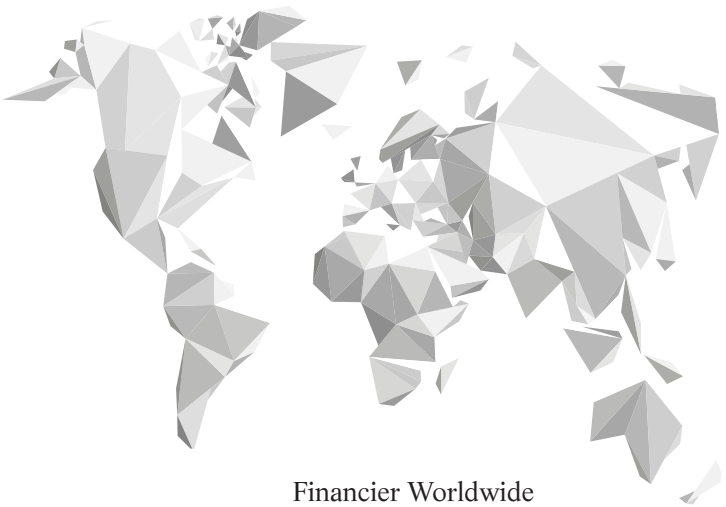
Financial crime, including money laundering, continues to plague the global economy, despite increased efforts by companies, regulators and financial institutions (FIs) to turn the tide.

Of course, over the last 12 months or so, the COVID-19 crisis has not helped. The impact of the pandemic has increased threat vectors – especially for FIs, by altering 'normal' red flags and complicating customer on-boarding and identification processes.

But FIs are far from the only parties affected by COVID-19. So much of our daily and working lives have moved online since the pandemic began, catching many companies underprepared. Undoubtedly, it has been a steep learning curve for many – shedding light on money laundering vulnerabilities.

As regulatory changes, new guidance and enforcement actions continue to mount, it is vital that organisations remain compliant and up to date with anti-money laundering (AML) regulations. Organisations need to consider all available tools at their disposal, including artificial intelligence, machine learning and robotic process automation, to enhance AML frameworks.

CONTENTS



Financier Worldwide canvasses the opinions of leading professionals on current trends in anti-money laundering.

UNITED STATES

Guidehouse

Respondent

SALVATORE R. LASCALA
Partner
Guidehouse
+1 (212) 554 2611
salvatore.lascala@guidehouse.com

Salvatore LaScala is a partner and Guidehouse's global investigations and compliance practice lead. Possessing a broad range of subject matter knowledge and expertise, he applies more than 20 years of hands-on experience to conduct investigations and compliance reviews on behalf of financial institution clients responding to regulatory or law enforcement matters concerning anti-money laundering (AML), Bank Secrecy Act (BSA), USA PATRIOT Act and Office of Foreign Assets Control (OFAC). He leads large teams that regularly perform historical transaction reviews, as well as know your customer (KYC), customer due diligence (CDD) and enhanced due diligence (EDD) file remediation work.

Guidehouse

Q. Could you provide an insight into recent trends shaping financial crime in the US? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Financial crimes, including money laundering and fraud, continue to pose a threat to financial institutions (FIs) across the US. 2020 was an unparalleled year for regulators, financial institutions and their customers. As of Q1 2020, the COVID-19 pandemic had caused shifts in the timing of regulatory examinations and the nature of regulatory guidance in the US and across the globe. Furthermore, FIs changed the way employees worked and had to swiftly put business continuity plans and other controls into action to protect data. The US saw only a brief pause in regulatory examinations during the early months of the pandemic and soon saw a return to normalcy as regulatory reviews and enforcement action teams adapted to working more remotely. In Q2 2020, the Federal Financial Institutions Examination Council (FFIEC) provided updated guidance to their Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual and in Q3 2020 the International Consortium of Investigative Journalists (ICIJ) Financial Crimes Enforcement Network (FinCEN) Files leak piqued the interest of the financial sector and federal bodies, shedding light on suspicious activity reports filed historically. In addition, the US has created partnerships with countries in the European Union (EU) on the provision of technical assistances in AML, counterterrorism and proliferation. These types of partnerships exemplify the common phrase 'international better practice'.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: There will always be bad actors leveraging illicit practices, particularly in times of need. Money laundering, human trafficking, elder abuse and sanctions exposure continue to be the main sources of risk for FIs. Moreover, all industries have seen increased incidences of fraud as a result of the changes in commerce and how we transact due to the pandemic. As a result, typical 'red flags' might look

Guidehouse

different and FIs will need to adjust transaction monitoring accordingly. For example, FI customers that typically transacted face-to-face now transact remotely and other processes, such as on-boarding and identification processes, are more valuable to identity theft and various online fraud typologies. This challenge relates to both banking and nonbanking institutions and payment processers which are also seeing significant increases in transactions and online merchant activity.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in the US? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: The ICIJ FinCEN Files have been an area of discussion in the US and worldwide. On 20 September 2020, the ICIJ FinCEN Files exposed previously filed suspicious activity reports (SARs) between 2000 and 2017. For many, this turn of events highlighted a need for discussion between regulatory bodies and the financial sector. On 16 September 2020, FinCEN announced solicitation of enhancing the effectiveness of AML programmes, welcoming questions and feedback "to potential regulatory amendments under the Bank Secrecy Act". Although institutions' involvement in reducing financial crime is ongoing, this suggests that the nature and extent of the demands being placed on companies is open for discussion. Moreover, cryptocurrencies and other alternative currencies continue to be a focus for US enforcement officials. The Financial Action Task Force (FATF) recently published guidelines for virtual currencies, however the US is still catching up. In 2020, there were enforcement actions against large FIs, law firms and individuals convicted of compliance failures and laundering through cryptocurrency exchanges.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Institutions must be proactive in reviewing and refreshing their compliance programmes. FIs should keep abreast of new enforcement actions, regulatory news and changes. Senior management, including the board of directors and

Guidehouse

compliance staff, should hold regular discussions regarding inefficiencies in the programmes or controls that are not working as anticipated. Ongoing training is vital in keeping up with the ever changing AML and sanctions landscape, particularly for the board of directors to nurture a culture of compliance throughout the organisation. This is especially relevant with respect to blockchain technology and crypto-related sanctions evasion typologies. Historically, the majority of regulatory fines issued in the US have been sanctions-related. In 2020, we saw examples of enforcement actions put into place for the first time, specifically with respect to broker-dealers and institutions offering convertible virtual currency services. Last year marked the first time in history that the Commodity Futures Trading Commission brought an action under 17 CFR § 42.2. Additionally, FinCEN announced the first-ever Bitcoin penalty in violation of AML laws.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

The Financial Action Task Force (FATF) recently published guidelines for virtual currencies, however the US is still catching up.

Guidehouse

A: As financial crimes become more complex and increase in scale, it is evident that technological solutions are here to stay. Artificial intelligence and machine learning (AI/ML) and robotic processing automation (RPA) technology have become exceedingly attractive in many institution's fight against financial crimes and evaluating solutions to enhance BSA, AML and sanctions oversight. AI/ML helps financial institutions bring to light key pockets of risk and vulnerabilities that were otherwise difficult to identify or emerging, and therefore potentially redirects their attention to areas of risk they did not previously have the ability to focus on. RPA allows institutions to more efficiently disposition alerts with the benefit of affording financial crimes specialists more time evaluating fraud and AML typologies than preparing investigative exhibits. Additionally, the use of blockchain analysis and crypto-tracing tools have been recent developments to assist with completing due diligence and enhancing transaction monitoring to trace the movement of virtual currency. It should be noted that technological enhancements may not be vital for an institution, depending on the size of the institution's compliance programme or risk exposure.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Once a financial institution determines that it has fallen victim to a financial crime, the business legal and compliance staff should immediately work with other employees to document the facts, convene the relevant committee of the board of directors and notify the appropriate regulatory or law enforcement agencies. Whether it is fraud, money laundering or a sanctions-related violation, the financial institution should undertake a root cause analysis and identify the weakness or absence of controls, including overall governance structure, that permitted the wrongful activity to occur. A renewed look at the risk assessment and a compliance programme gap analysis should also be undertaken to determine the precise programme control and process weaknesses. Such analyses might include a skills assessment of staff and an accountability and oversight investigation, if warranted. Many institutions have

Guidehouse

integrated the approach to fighting financial crime and by consolidating fraud, AML and other criminal investigations to ensure that each discipline shares knowledge seamlessly and to consolidate similar governance and control structures.

Q: What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: It is important for institutions to stay well informed with respect to regulatory changes, particularly when regulatory change is imminent. Institutions should also prioritise critical matters and reassess priorities throughout the year and revisit their risk assessments and risk tolerances to ascertain whether they are measuring financial crime risk and the counterbalancing effect of financial risk controls effectively.❑

www.guidehouse.com

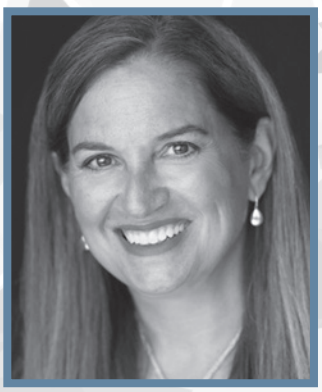
GUIDEHOUSE is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology and risk consulting. The firm helps clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology and analytics services, Guidehouse helps clients create scaleable, innovative solutions that prepare them for future growth and success.

SALVATORE R. LASCALA Partner
+1 (212) 554 2611
salvatore.lascala@guidehouse.com

CANADA

Deloitte LLP

Respondents



CHRISTINE RING
Partner
Deloitte LLP
+1 (416) 775 8851
cring@deloitte.ca

Christine Ring is a partner in Deloitte's financial crime practice, focusing on anti-money laundering and sanctions for Deloitte Canada. She brings over 20 years of regulatory experience, including vast experience in financial crime and anti-money laundering compliance, as the former managing director of the Office of the Superintendent of Financial Institution's (OSFI's) AML and Compliance Division. She holds a law degree from the University of Western Ontario and is a member of the Law Society of Upper Canada. She also holds a designation from the Association of Certified Anti-Money Laundering Specialists.

MICHAEL CHAU
Partner
Deloitte LLP
+1 (416) 601 6722
michau@deloitte.ca

Michael Chau is a partner in Deloitte's financial crime practice focusing on anti-money laundering and sanctions for Deloitte Canada. He brings over 15 years of experience assisting leading Canadian financial institutions on regulatory transformations focused on the translation of regulations into compliant and optimised operational capabilities. He has advised on the strategic end-to-end design and implementation of the largest anti-money laundering and sanctions programmes in Canada, including strategic operating model, business process, technology and data. He is a graduate of the Schulich School of Business, York University and is a Chartered Financial Analyst charterholder.

Deloitte LLP

Q. Could you provide an insight into recent trends shaping financial crime in Canada? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Canada's anti-money laundering (AML) regulatory regime is continuously evolving to respond to financial crime risks. At the federal level, the AML regulatory regime establishes a common set of requirements covering multiple industries, such as financial services, casinos and real estate, and the federal government announced funding to establish new AML law enforcement units in Canada's four largest provinces. Some provinces have recognised the need to implement their own unique requirements to address provincial AML-related vulnerabilities. Financial crime perpetrators have exploited vulnerabilities in Canada's regulatory regime and trends in consumer behaviour, such as increasing adoption of digital means to conduct transactions. Despite recent amendments to the legislative requirements – the Proceeds of Crime, Money Laundering and Terrorist Financing Act (PCMLTFA) and increased regulatory scrutiny on high-risk sectors other than financial services, there continues to be vulnerabilities related to beneficial ownership, intelligence sharing among regime stakeholders, and lawyers as a reporting entity. To date, regulatory supervision has focused on Canadian financial institutions (FIs), resulting in more mature AML programmes and greater investment of resources. It is increasingly important for Canada to promote greater integration between government departments and public-private partnerships to effectively manage financial crime risk.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Prosecution of money laundering is linked to predicated offences, as defined in the Canadian Criminal Code. Transactions should be identified by regulated organisations and reported to Canada's AML Financial Intelligence Unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), where financial crime is connected to money laundering. FINTRAC has issued guidance bulletins to regulated entities

Deloitte LLP

FINTRAC and the Canadian government have ongoing consultations with regulated entities to clarify reporting changes – a positive 'public-private' approach.

on topics ranging from money laundering indicators associated with online child sex exploitation, casino-related underground banking schemes and risk indicators for dealers in precious metals and stones. FINTRAC's guidance includes factors that entities should be aware of related to AML in those scenarios, such as common transaction patterns, client profiles and payment methods. In addition, current industry topics of focus for Canadian FIs include drug and human trafficking, child exploitation and money laundering through real estate.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Canada? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Canada has recently made changes to its AML regulatory requirements, including suspicious transaction and electronic funds transfer reporting requirements. These changes significantly expand the obligations on reporting entities with respect to the breadth of data that will be required for reporting to FINTRAC with

the goal to improve intelligence available to law enforcement. Many of Canada's FIs have established large business and technology programmes to make necessary technology, data and business process changes. FINTRAC and the Canadian government have ongoing consultations with regulated entities to clarify reporting changes – a positive 'public-private' approach. At the provincial level, British Columbia (BC) has taken significant strides to uncover the extent of money laundering through the establishment of the Cullen Commission, an independent inquiry forum designed to make its own findings and recommendations regarding money laundering in the province. BC also established a new land registry with the goal of improving transparency of the real estate market and combatting money laundering. The outcomes of the initiatives in BC may encourage further action at the federal level.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Historically, FINTRAC has issued limited AML monetary penalties against Canada's FIs and other regulated entities. Examinations conducted by Office of the Superintendent of Financial Institutions (OSFI), the federal prudential regulator, and FINTRAC have resulted in entities committing to address deficiencies by establishing comprehensive action plans with key milestones. Like most countries, Canada requires regulated entities to assess the effectiveness of their AML programmes on an ongoing basis. FIs commonly rely on a three lines of defence model and seek support from third-party experts where technical competencies may be lacking. In addition, changes to AML practices are informed through ongoing interactions with OSFI and FINTRAC. Even in the absence of possible enforcement action, FIs are expected to proactively manage their money laundering risk and look for opportunities to enhance their practices by optimising how technology is used in their end-to-end AML processes.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

Deloitte LLP

A: Effective use of technology and analytics is necessary to combat financial crime and reduce ongoing operational costs of financial crime programmes. Examples of technology and analytics enablers include machine learning algorithms in transaction monitoring rules to reduce false positives, robotic process automation (RPA) to optimise investigative processes and reduce repetitive tasks, networks and entity-resolution to visualise risk areas, enhanced use of reporting and advanced analytics and consolidation of disparate datasets to produce a 360-degree view of the customer. For large FIs, big data and analytics are rapidly becoming a critical capability to manage financial crime. Companies are exploring financial crime fusion – how to integrate AML with other financial crime functions, such as fraud.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Financial crime must be reported to regulatory authorities as soon as practicable if it is connected to money laundering. Many companies also report financial crime to law enforcement and update their 'do not do business with' lists to prevent future business relationships with customers who have committed these offences. It is critical for companies to understand financial crime trends and the specific risks they are facing, such as the behaviours and risks posed by customers and the vulnerabilities of the company's products channels and geographies to financial crime. These data points should be proactively analysed so that companies can enhance their technology capabilities and processes to better detect and deter financial crime. Regulated entities and regulators should have strong bilateral relationships, proactively communicate expectations and share intelligence and understand trends, for the active management of AML risk.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: Companies use multiple levers to improve the effectiveness of their financial

Deloitte LLP

crime risk management programmes, such as integrating new technologies into their process, enhancing their process delivery models and leveraging data. Given that the AML aspect of financial crime programmes is subject to regulatory oversight, the AML programme must include appropriate governance and oversight mechanisms and a strong 'tone from the top'. As companies invest in technology, process changes and data enhancements to improve their programmes, it is important to ensure these enabling capabilities are underpinned by supportable and right-sized risk methodology designs. Greater integration of financial crime programmes within FIs is evolving through the exploration of sharing infrastructure and capabilities across business and risk domains, such as analytics, case management and customer on-boarding, with the view to enhancing and optimising financial crime risk management programmes.❑

www.deloitte.ca

DELOITTE provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500 companies through a globally connected network of member firms in more than 150 countries and territories, bringing world-class capabilities, insights and service to address clients' most complex business challenges. Deloitte LLP is the Canadian member firm of Deloitte Touche Tohmatsu Limited, which is a network of member firms, each of which is a legally separate and independent entity.

CHRISTINE RING Partner
+1 (416) 775 8851
cring@deloitte.ca

MICHAEL CHAU Partner
+1 (416) 601 6722
michau@deloitte.ca

Deloitte.

BRAZIL

FTI Consulting

Respondents

DAIANE NABUCO
Senior Director
FTI Consulting
+55 11 3165 4535
daiane.nabuco@fticonsulting.com

Daiane Nabuco is senior director in the global risk and investigations practice within the forensic and litigation consulting team, based in São Paulo. With more than 12 years of auditing experience, she works with large corporations on projects that seek to identify potential operational risks, inadequate management and vulnerable points that could generate financial risks for the company. Prior to joining FTI Consulting, she worked at Grant Thornton and Ernst Young in fraud, investigation and disputes. She was also responsible for structuring the internal audit department at CPFL Renováveis, a large Brazilian renewable energy company.

RÉGIS PEREIRA
Senior Director
FTI Consulting
+55 11 3165 4535
regis.pereira@fticonsulting.com

Régis Pereira is a senior director in the global risk and investigations practice within the forensic and litigation consulting team, based in São Paulo. With more than 15 years of technology consulting experience, Mr Pereira usually focuses on leading complex e-discovery efforts and conducting detailed computer forensics. He regularly assists clients in all phases of investigations, helping them understand their options when responding to government subpoenas and counterparts' requests. In 2019 and 2020 he was recognised as a 'Future Leader for Digital Forensic Experts' by Who's Who Legal.

FTI Consulting

Q. Could you provide an insight into recent trends shaping financial crime in Brazil? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Financial crime trends in Brazil are directly related to cyber crime. In this regard, the financial market and the banking sector are the industries that suffer the most from these attacks. The most common financial crimes, such as money laundering and tax evasion, have become more sophisticated with the advancement of technology. The banks, for example, increasingly use compliance tools to automate the processes of combatting and preventing fraud, money laundering and privileged information leaks. Brazil is already one of the most impacted countries with respect to money laundering, but despite the large number of cases, including cases that were investigated under the *'Lava Jato'* investigation, the country is far from being a tax or legal haven. The country has many rules, including regulatory rules, related to money laundering. The Brazilian Central Bank and other institutions that regulate the financial sector, such as the Council for Financial Activities Control (COAF), have measures to monitor and prevent money laundering activities, such as communication which indicates illegal activities as described in Law 9,613/98, financial institutions monitoring, intelligence reports and the communication of automatic transactions and those of high value.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: According to surveys carried out by technology companies in Brazil, one in three entities have fallen victim to a financial crime. This is a growing trend, and as technology evolves and digital resources become increasingly available, the sophistication and threat level of criminals has continued to escalate. Today, electronic fraud and cyber attacks are the most common threats that companies face in Brazil. Financial crimes such as leaking privileged information in purchase and sales transactions, insider trading and credit card fraud, among others, are the most common crimes perpetrated

FTI Consulting

in Brazil. For experts, the source of this risk is associated with companies' poor monitoring of digital and virtual environments and customer data, as well as unprotected systems and a lack of specific training to combat the spread of these crimes.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Brazil? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Financial crime is a major global threat which causes financial losses in the trillions of dollars worldwide. One of the main regulatory and legal initiatives in recent years was the introduction of the General Data Protection Regulation (GDPR) in the European Union (EU), and the General Data Protection Law (LGPD) recently approved in Brazil. The LGPD aims to protect Brazilian citizens against violations of their privacy and data, and thus prevent digital crimes. Companies are more attentive to these types of crimes, and with new regulatory initiatives such as the LGPD, they will need to more frequently assess their vulnerabilities, whether the organisation has handled its information properly, potential employee responsibilities, and the consequent regulatory fines and penalties that the company may suffer. In addition to the LGPD, which covers not only the financial market but all of Brazilian society, today there are regulatory initiatives aimed at preventing and mitigating financial risks, such as financial compliance that regulates issues related to money laundering, and the commercial trade compliance laws. It is also important to mention Brazilian Money Laundering Law 9,613/98 which contains specific regulations to combat and prevent money laundering.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Historically, companies tend to invest more in reactive measures than in preventing illicit acts. Companies should not only review their practices and evaluate them for effectiveness periodically and proactively, but also establish formal monitoring criteria and actions to mitigate any threats, at the highest level of the

FTI Consulting

administrative chain. Best practice is for each company to establish a monitoring plan to combat and prevent financial crimes, and to conduct this assessment regularly. Some departments, such as internal audit and compliance, play a fundamental role in this prevention process. Acting based on these results and in a transparent manner can improve the perceived lack of impunity for those who act illegally.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Cyber crime happens at a frightening frequency due to the advent of the internet and technology. Today, information security is a serious and ongoing problem faced by several countries and organisations. However, technology is an indispensable tool for combatting and investigating financial crimes. In Brazil, for example, there is an initiative led by the Federal Police and the Brazilian Banks Federation (Febraban) to prevent electronic banking fraud which includes debit card, credit card, internet banking,

Companies should invest in technological tools designed to ensure financial crime compliance and to monitor constantly evolving regulations.

FTI Consulting

call centre and electronic bank slip frauds committed by criminal organisations. According to experts in the banking sector, banking technology has advanced significantly, and financial institutions have interconnected systems that automatically forward information to the Federal Police with important details of the investigation. With regard to money laundering, in addition to the monitoring carried out by municipalities and regulatory bodies such as the Brazilian Central Bank and COAF, Brazil has a national strategy to prevent corruption and money laundering that relies on the interaction of several public officials and public control, inspection, legal and strengthening bodies of the Brazilian financial system.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Financial crimes can spread quickly in organisations due to rapid advancements in technology. In many cases, companies find that they are being used for financial crime and they are being financially harmed long after the first crime was committed. When faced with this situation, organisations must first establish a specific team or committee, if one does not exist, to initiate an internal investigation. Depending on the magnitude of the crime, this process can be done internally or with the support of third-party companies. It is also important to assess the information security environment of the organisation, the chain of approval that involves financial resources, systems and interactions between departments, to ensure that these areas and activities are carried out in accordance with the company's code of ethics. The results of these actions must reflect the company's level of transparency and its concern with compliance and governance best practices, and the applicable sanctions and penalties, previously established in internal policies and procedures, must be applied to those individuals involved in criminal activities, in order to demonstrate that the company does not tolerate such practices.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

FTI Consulting

A: Companies should invest in technological tools designed to ensure financial crime compliance and to monitor constantly evolving regulations. Currently, there are tools that act efficiently in the fight against money laundering, bribery and corruption, as well as cyber attacks and related crimes. The company must also assess its stakeholders' adherence to financial crime compliance requirements, identify gaps in their processes and improve due diligence workflows associated with current legislation, and imposed by oversuight bodies and economic sanctions.❑

www.fticonsulting.com

FTI CONSULTING is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes. Individually, each practice is a leader in its specific field, staffed with experts recognised for the depth of their knowledge and a track record of making an impact. Collectively, FTI Consulting offers a comprehensive suite of services designed to assist clients across the business cycle – from proactive risk management to the ability to respond rapidly to unexpected events and dynamic environments.

DAIANE NABUCO Senior Director
+55 11 3165 4535
daiane.nabuco@fticonsulting.com

RÉGIS PEREIRA Senior Director
+55 11 3165 4535
regis.pereira@fticonsulting.com

UNITED KINGDOM

Grant Thornton

Respondents

THOMAS TOWNSON
Partner
Grant Thornton
+44 (0)20 7865 2175
thomas.f.townson@uk.gt.com

Tom Townson has over 20 years' experience as a practitioner and as a consultant to financial service firms in the financial crime arena, covering fraud, anti-money laundering (AML), sanctions, AB&C and conduct issues. He has led a number of globally significant programmes concerned with advising on building, reviewing or improving financial crime frameworks primarily at firms subject to intensive regulatory scrutiny involving multiple jurisdictions and regulators.

DAVID SOWDEN
Director
Grant Thornton
+44 (0)7831 521524
david.sowden@uk.gt.com

David Sowden is a forensic accountant with over 25 years' experience of investigating international corruption, fraud and money laundering matters. He has given evidence in the Royal Court in Jersey, the Royal Court in Guernsey and in the Crown Court in England, as well as assisting with criminal investigations in the Isle of Man and for the Scottish Ministers. He also acts on regulatory investigations and assists with complex multijurisdictional insolvency investigations. Three of his cases feature in Financial Action Task Force (FATF) typology reports.

Grant Thornton

Q. Could you provide an insight into recent trends shaping financial crime in the UK? How great a risk does financial crime, such as money laundering, now pose to companies?

A: The UK National Risk Assessment, published December 2020, identified diverse methods being used by criminals to exploit the global financial system, often facilitated by professional services providers such as accountants, lawyers and trust and corporate service providers. A similar Jersey publication in 2020 identified the island's main risks as heavily influenced by the sectors and jurisdictions in which key business is conducted. The dominance of the Trust and Company Service Provider (TCSP) and banking industries in Jersey place it at a greater risk of money laundering, and the vulnerabilities in the domestic regimes of other jurisdictions allow criminality to occur elsewhere and the proceeds transferred to or through Jersey. Difficulties include verifying the source of wealth, source of funds and politically exposed persons (PEPs) where potentially linked to bribery and corruption. In our experience, the difference between source of wealth and source of funds is not always understood and remains a key focus for regulators.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Cyber crime is a key means for criminals to target organisations and a startling proportion of companies will have fallen victim to cyber crime. High-profile ransomware attacks have received press coverage, but many more go unreported. The lack of preparation by some organisations to adequately protect themselves, and the relative ease with which tools are available to perpetrate such attacks, means organisations are at risk from tech-savvy operators. Cyber-enabled fraud is increasing the scale of some financial crimes and the speed with which they can be perpetrated. During the coronavirus pandemic, increased online activity created more opportunities for criminals to perpetrate fraud. Payment diversion frauds can target different organisations at one time and provide links to mirror websites to add

Grant Thornton

While technology has undoubtedly been exploited by criminals, recent advancements are now showing the vital role technology can play in law enforcement and fighting financial crime.

apparent legitimacy to the request, duping companies into unwittingly diverting money to the fraudster's bank account. Financial services and telecommunications are sectors where collaboration is required to counter this threat.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in the UK? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: In previous years there was an emphasis on developing robust anti-money laundering/combatting the financing of terrorism (AML/CFT) policies and regulation. Increasingly, regulators are now looking to move toward a more aggressive enforcement policy. The Financial Conduct Authority's (FCA's) 2020/21 Business Plan covers a number of challenges ahead, not least the impact of the COVID-19 pandemic and leaving the EU. Alongside such issues, the FCA is also focused on the importance of culture, including looking at leadership, purpose, governance, management and employee reward. We also expect regulatory focus will shift to

Grant Thornton

smaller firms and to firmer action being taken against firms which consistently fail to meet the required standards. This approach is being mirrored in the Channel Islands. We anticipate regulators will be particularly focusing on areas such as governance, KYC, enhanced due diligence, negative news and sanctions screening, transaction monitoring, training, codification of framework through policies and procedures, and suspicious activity reporting, so organisations need to be prepared for this.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: In our view, proactively reviewing and revising internal practices is essential and all companies need to be mindful of their risk exposure. A recent enforcement action in Guernsey against a TCSP which assisted in setting up luxury asset-holding companies for ultra-high net worth individuals, some of whom had previously been involved in illegal activities, resulted in fines for the company as well as for individual directors and the money laundering reporting officer (MLRO). In this instance, the firm had failed to conduct proper risk assessments, comply with the termination of identified high risk business, and establish and maintain appropriate and effective procedures and controls to prevent and detect money laundering and terrorist financing. The issues uncovered in this inspection are not unique. These failings often arise from a poor internal culture, a common feature of which is inadequate oversight mechanisms, and a failure to properly invest in training for all levels of staff.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: While technology has undoubtedly been exploited by criminals, recent advancements are now showing the vital role technology can play in law enforcement and fighting financial crime. Artificial intelligence (AI) is now more widely accessible to tackle financial crime with off-the-shelf packages available which are constantly being refined with each new iteration utilising previous learning. Fertile areas for development are those

Grant Thornton

where there is currently heavy deployment of staff, such as customer and payment screening and transaction monitoring. We see the benefits, both in time and cost, of using AI packages to perform analysis work. Once the software has identified what is 'normal' activity in a particular dataset, the technology can then be used to find patterns, statistical links and relationships in the dataset that may not have been identified through traditional manual review.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Time is of the essence. Fraudsters plot the extraction of funds so that they are difficult to recover with financial systems making it relatively easy for money to be transmitted quickly around the world, posing challenges for tracing, freezing and recovering funds. Organisations must act quickly by contacting their own bank in the first instance. The deployment of accountants, lawyers and consultants to assist with recovery may be required. Lawyers will help with court orders, accountants can trace the funds and consultants can advise on the root cause of the fraud and on future prevention. Cyber expertise may be required where there has been large data loss. The trigger event is often the tip of the iceberg. Firms need to establish the motive of the fraudster and what other losses may have occurred. Firms also need to be mindful of any statutory reporting obligations they may face.

Q: What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: Firms should regularly evaluate their risk appetite and ensure all employees are aware of this and should encourage challenges from all levels of staff. As such, they should not underestimate the value of regular updates and refresher training on the basics for all employees. It is all too easy for complacency to creep in, relationships to become too familiar, and corners to start being cut. Setting the tone for this needs to come from the top of the organisation. Consideration is needed as to

Grant Thornton

who you are doing business with and why. Ask yourself if the customer is somebody you want your company to be associated with and whether you are comfortable with the transactions you are being asked to be a part of. Finally, especially for regulated firms, be disciplined about documenting and evidencing decisions and how they were arrived at, as this is critical to good governance.❑

www.grantthornton.co.uk

GRANT THORNTON UK LLP is part of the Grant Thornton network of independent assurance, tax and advisory firms in over 135 countries. For more than 100 years, the firm has helped dynamic organisations realise their strategic ambitions. Whether you are looking to finance growth, manage risk and regulation, optimise your operations or realise stakeholder value, Grant Thornton can help you. The firm has got scale, combined with local market understanding. That means they are everywhere you are, as well as where you want to be.

THOMAS TOWNSON Partner
+44 (0)20 7865 2175
thomas.f.townson@uk.gt.com

DAVID SOWDEN Director
+44 (0)7831 521524
david.sowden@uk.gt.com

ANGELA ROBERTS Manager
+44 (0)113 200 1678
angela.h.roberts@uk.gt.com

Grant Thornton
An instinct for growth™

IRELAND

Dillon Eustace

Respondent

KEITH WAINE
Partner
Dillon Eustace
+353 (1) 673 1822
keith.waine@dilloneustace.ie

Keith Waine is head of the financial regulation team at Dillon Eustace and provides regulatory advice to domestic and international financial service providers, including banks, insurers, broker-dealers, asset managers, payment firms, crypto asset service providers and other regulated and unregulated businesses. He has extensive experience advising clients in relation to their most complex AML/CFT issues and previously served as head of legal and compliance with responsibility for AML/CFT at a full-service Irish bank. He is an active member of the Association of Compliance Officers in Ireland and a frequent author and speaker on financial regulatory topics.

Dillon Eustace

Q. Could you provide an insight into recent trends shaping financial crime in Ireland? How great a risk does financial crime, such as money laundering, now pose to companies?

A: As a substantial and expanding international hub for financial services, Ireland's exposure to and risk from financial crime is significant and increasing. Data from the Central Statistics Office shows that there were 7832 recorded incidents of fraud, deception and related offences in the year to September 2020. This was 0.8 percent down on the year to September 2019 but followed a 35 percent increase on the previous year. Rapid technological developments, particularly in the areas of online financial services, payment infrastructures and cryptoassets, have created new opportunities for criminals. Added to that, the disruption to the financial system caused by the pandemic is being exploited by criminals to mask money laundering and terrorist financing. In particular, there has been an increase in cyber crime, made possible by the weaker security defences of companies that have adopted working from home arrangements. The Irish police published a scam warning at the beginning of the pandemic, highlighting increased risks around 'phishing' and associated frauds, fraudulent selling and social engineering scams. The risks arising from financial crime are not limited to financial loss. Companies hit by financial crime may also face regulatory sanction and significant reputational damage. At a macro level, failure to adopt effective measures to prevent, detect and prosecute financial crime is likely to damage Ireland's standing as a financial services centre.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Cyber crime is currently the most prevalent type of financial crime reported by Irish companies. A recent report published by PwC following a survey of Irish and global companies showed incidences of cyber crime in Ireland to be double that experienced by global companies. On 8 October 2020, the Department of Justice and Equality published a report on cyber crime and the Irish anti-cyber crime landscape. The

report notes that the most significant cyber crime trends and threats currently include ransomware and other malware threats, data breaches and network attacks, spearphishing – targeting specific individuals for the purposes of distributing malware or extracting sensitive information – and attacks against critical infrastructure. Other types of fraud commonly occurring in Ireland include payment card fraud, invoice redirection fraud, a form of social engineering called chief executive fraud, telephone fraud known as 'vishing' or 'smishing', and advance fee fraud, where criminals target victims to make upfront payments for goods or services that do not materialise. Key vulnerabilities for organisations are the absence of clear and effective policies and procedures and failure to adequately train and empower staff to detect and prevent fraudulent activity.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Ireland? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: As a member of the European Union (EU), Ireland is currently in the process of implementing the EU's Fifth Money Laundering Directive (5AMLD). The new legislation will extend the scope of anti-money laundering (AML) requirements to new categories of businesses, including virtual asset service providers, custodian wallet providers, letting agents and art dealers. 5AMLD, which Ireland is late in implementing, also makes a number of targeted enhancements to the legislative framework in areas such as anonymous prepaid cards, due diligence on high-risk third countries and cooperation with other EU member states. Ireland has already implemented central registers of beneficial ownership of corporates and certain investment fund vehicles. A central register of beneficial ownership of trusts is expected to be established later this year. Further changes are expected on foot of the European Commission's action plan for a comprehensive EU policy on preventing money laundering and terrorist financing, which was adopted in May 2020. In December 2020, the report of the Governmental Review Group on anti-fraud and anti-corruption was published. The report makes a

Dillon Eustace

number of recommendations designed to enhance Ireland's framework for tackling economic crime and corruption, including recommendations for legislative changes, structural and systemic changes, and increased resources.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Given the current legislative and regulatory focus on financial crime, businesses can expect increased compliance demands in areas such as anti-bribery and corruption, AML, lobbying and fraud prevention. The Central Bank of Ireland has taken a number of enforcement actions in relation to AML compliance failures in recent years. We expect that trend to continue and for there to be an increase in enforcement activity in respect of other financial crimes.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

The Central Bank of Ireland has taken a number of enforcement actions in relation to AML compliance failures in recent years. We expect that trend to continue.

Dillon Eustace

A: Technology can assist businesses in identifying areas of risk and allow them to be more focused in their efforts to combat financial crime. Advanced analytics may help companies to identify trends and patterns indicative of financial crime that are not otherwise easily discernible. The use of transaction monitoring systems is widespread in Ireland and is increasing in line with the increasing volume and speed of transactions. The Central Bank of Ireland has recently set out its expectations in this area, which include an expectation that transaction monitoring systems are tailored to fit the company's business risk assessment and are capable of being configured to reflect changing risks over time. The Central Bank notes that while the use of an automated transaction monitoring solution is desirable, companies should not place absolute reliance on any such system and employees should be aware of the need to manually identify suspicious transactional activity.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: As well as taking steps to prevent the occurrence or recurrence of the incident, a company needs to consider its various reporting requirements. The nature of those requirements will vary depending upon the regulatory status of the company. It should be noted, however, that it is an offence under Irish law for any company or individual not to report information that might be of material assistance in preventing the commission of a financial crime or in securing the apprehension, prosecution or conviction of a person for such a crime. Companies also need to ensure that they have a process in place for informing affected clients, while being cognisant of the requirement not to tip off the perpetrator of the incident.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: One of the first steps should be identifying and assessing the company's financial crime risks and vulnerabilities. This is key to designing a risk management

Dillon Eustace

framework with a focus on prevention and early detection of incidents. Companies should ensure that their policies, procedures and controls are up to date and fit for purpose. Bear in mind that regulators are increasingly looking for a key individual, such as the head of compliance, to have overarching responsibility for financial crime matters. Outsourcing arrangements should also be reviewed, and enhanced assurance testing implemented where appropriate. Companies should ensure that all technologies employed are subject to regular review and compliance assurance testing. Transaction monitoring systems should be tailored to identify red flags applicable to the company's clients and activities. Where appropriate, companies should consider the use of data analytic tools to enhance their monitoring capabilities.❑

www.dilloneustace.com

DILLON EUSTACE is one of Ireland's leading law firms focusing on financial services, banking and capital markets, corporate and M&A, litigation and dispute resolution, real estate and taxation. Headquartered in Dublin, the firm has offices in Cayman, New York and Tokyo. In tandem with Ireland's development as a leading international financial services centre, Dillon Eustace has developed a dynamic team of lawyers representing international and domestic asset managers, investment fund promoters, insurers, banks, corporates, TPAs and custodians, prime brokers, government and supranational bodies as well as newspapers, wind energy companies, aviation and maritime industry participants and real estate developers.

KEITH WAINE Partner
+353 (1) 673 1822
keith.waine@dilloneustace.ie

SWITZERLAND

Wenger & Vieli Ltd.

Respondents

DANIEL S. WEBER
Counsel
Wenger & Vieli Ltd.
+41 (58) 958 53 27
d.weber@wengervieli.ch

Daniel Weber is a counsel and member of Wenger & Vieli's financial services group specialising in banking and regulatory matters, including the new Financial Services Act (FinSA) and Financial Institutions Act (FinIA), asset management and investment funds, FinTech, compliance, internal and regulatory investigations and white-collar crime. He represents clients in proceedings before the Swiss Financial Market Supervisory Authority (FINMA), the SIX Swiss Exchange and the CDB Supervisory Board. As a former deputy head of investigations at a major Swiss bank and as a secondee in the enforcement division of FINMA, he has broad experience in solving complex regulatory and compliance matters.

MICHAEL MRÁZ
Partner
Wenger & Vieli Ltd.
+41 (58) 958 58 58
m.mraz@wengervieli.ch

Dr Michael Mráz's practice focuses on white-collar crime, international judicial and mutual administrative assistance, as well as on matters relating to the Swiss Financial Market Supervisory Authority (FINMA). He specialises in advising and representing clients in criminal and regulatory proceedings. Dr Mráz represents individuals and companies involved in criminal proceedings, as well as those harmed by a criminal offence. Another focus of his work is providing advice and support to clients in their compliance and prevention efforts as well as internal investigations.

Wenger & Vieli Ltd.

Q. Could you provide an insight into recent trends shaping financial crime in Switzerland? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Switzerland is a leading global cross-border wealth management hub for private clients. This makes it particularly exposed and vulnerable to financial crime and money laundering. In November 2020, the Swiss Financial Market Supervisory Authority (FINMA) published its annual Risk Monitor, which provides an overview of what it believes are the most important risks currently facing Swiss financial institutions (FIs), and money laundering continues to feature heavily. Owing to shrinking profit margins, FIs may pursue relationships with profitable new clients from high-risk emerging-market countries where there is a serious threat of corruption. Many recent global corruption and AML scandals have all had links to Switzerland and its banking system. The numerous violations of anti-money laundering (AML) regulations by FIs and other gatekeepers in the wake of these scandals show that the risks involved in the cross-border wealth management business remain high. In addition to the traditional AML risks, FIs also face emerging risks in the area of blockchain technology and in relation to digital assets.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Financial flows associated with corruption and embezzlement can not only be linked to just private clients, who often qualify as politically exposed persons (PEPs), but also to state or quasi-state organisations and sovereign wealth funds. Money laundering risks are increased further by complex structures that impair transparency when it comes to identifying the beneficial owners of the assets concerned. These structures include domiciliary companies, fiduciary relationships and insurance wrappers.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Switzerland? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

Wenger & Vieli Ltd.

Enforcement of AML compliance continues to be a top priority for regulators around the world, which is why FIs must get it right and meet the enhanced regulatory requirements.

A: In 2016, the Financial Action Task Force (FATF) Mutual Report identified a range of weaknesses in Switzerland's AML framework. As a result, Switzerland is engaged in an enhanced follow-up procedure. To exit this procedure, it started to implement several changes to its AML framework. For instance, FINMA revised its Anti-Money Laundering Ordinance (AMLO-FINMA), which came into force on 1 January 2020 and was adjusted on 1 January 2021 to implement changes from the new Financial Services Act (FinSA) and the Financial Institutions Act (FinIA). The amended AMLO-FINMA sets out in more detail the requirements for global monitoring of AML risks. It also specifies the risk management measures which must be put in place if domiciliary companies or complex structures are used or if there are links to high-risk countries. To meet the FATF requirements, the Swiss Anti-Money-Laundering Act (AMLA) is currently under revision. The revised AMLA is expected to enter into force 1 January 2022 at the earliest. The proposed draft stipulates the explicit duty of FIs to check the details of the beneficial owner and to perform regular risk-based reviews of whether the client documentation is

up to date. Further, advisory services including foundation, acquisition, disposal, administration and funding of domiciliary companies with registered offices in Switzerland or abroad and trusts will be subject to the AMLA requirements. At the same time, due diligence, auditing and reporting obligations for 'advisers' shall be introduced.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Enforcement of AML compliance continues to be a top priority for regulators around the world, which is why FIs must get it right and meet the enhanced regulatory requirements. Both FINMA and the self-regulatory organisations seek to prevent money laundering. In recent years, both FINMA and prosecutors investigated several cases where FIs domiciled in Switzerland breached regulatory and criminal laws in their handling of certain client relationships. During FINMA's investigations at several Swiss banks, it discovered systemic failures to comply with due diligence requirements under AMLA, as well as violations of AML reporting requirements. FINMA imposed various mitigation measures. One bank was even prohibited from conducting major acquisitions that would lead to a significant increase in operating risks or in its organisational complexity until it is once again fully compliant. While FINMA stated that it has most recently and in general observed higher standards of compliance with the legal obligations to combat money laundering, FIs should assess and enhance the robustness of their AML framework and training on an ongoing basis.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: The implementation of IT-based solutions, such as sophisticated transaction-monitoring systems or the use of smart data analytics tools is best practice and assists FIs to better detect, manage and prevent risks arising from potentially suspicious transactions. Innovative technology helps connect the dots, for example the huge volumes of data across domains, to provide

Wenger & Vieli Ltd.

compliance specialists with more complete and targeted information, rather than restricting monitoring to individual transactions or clients. FIs should correctly embed the AML tools within their relevant day-to-day activities to enhance the efficiency of their AML capabilities and to allow them to swiftly detect unusual behaviour and identify red flags. FIs should also deploy more data-driven validation of machine learning models to increase trust in currently used algorithms and enable the development and acceptance of advanced surveillance systems. Also, clients need to be onboarded and screened efficiently while complying with the AML regulations. IT-supported risk assessments and approvals, such as for PEPs or other high-risk relationships, significantly speed up compliance with AML regulations.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: The AMLA specifies the procedures an FI must follow if it suspects assets might be tainted. The provisions governing special duties of due diligence, as outlined in Article 6 of the AMLA, require FIs to clarify the economic background and purpose of a transaction or business relationship if it appears unusual or suspicious. The investigations carried out must be documented to enable third parties to reach a well-founded judgement on the transaction or business relationship and establish whether it complies with AMLA. 'Reasonable suspicion' exists when the results of these clarifications fail to refute the suspicion that the assets are linked with a crime. The FI must report such business relationships to the Swiss Money Laundering Report Office, under Article 9 AMLA – reporting duty. If it is unclear whether a report must be filed, the FI may still do so – reporting right.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: An FI's AML framework must be adapted in line with its risk appetite, product portfolio and geographical coverage. FIs need to improve their surveillance and mitigation systems

continuously and in a holistic way. Given the major changes in the compliance and regulatory landscape and the resulting long-term impact on FIs, incremental adjustments will not be enough. FIs should design a new approach that integrates operational and compliance risk programmes. These programmes should be coordinated and follow a consistent standard and single platform. Integrated reporting and analytics provide compliance and management with a constructive, single view of risk. Products and channels are continually assessed from multiple perspectives and adjustments are made when needed. Further, compliance processes are subject to continuous improvement. Finally, the combined analysis of structured and unstructured data is forward-looking and shapes the compliance agenda for upcoming risk assessments, monitoring and other framework components.❑

www.wengervieli.ch

WENGER & VIELI LTD. is a nationally and internationally active law firm with offices in Zurich and Zug, Switzerland. For 50 years, the firm has been advising and representing national and international companies as well as private clients residing in or outside Switzerland primarily in all areas of business and tax law. Providing advice on a personal level and having small teams attend to its clients allows the firm to respond quickly and individually to particular needs. Wenger & Vieli advises its clients in German, English, French, Italian, Spanish, Czech and Russian.

DANIEL S. WEBER Counsel
+41 (58) 958 53 27
d.weber@wengervieli.ch

MICHAEL MRÁZ Partner
+41 (58) 958 58 58
m.mraz@wengervieli.ch

DR MARTIN PEYER Counsel
+14 (58) 958 53 53
m.peyer@wengervieli.ch

wenger & vieli
Attorneys at law

GERMANY

PwC

Respondent

LARS-HEIKO KRUSE
Partner
PwC
+49 302 636 2006
lars-heiko.kruse@pwc.com

Lars-Heiko Kruse is a partner in PwC's forensic services practice. He leads the banking capital markets group within the forensics practice. Since 2003, he has advised PwC customers regarding the implementation of the regulatory guidelines and standards with regard to anti-money laundering, terrorist financing, financial sanctions violations and other criminal offences. He is responsible for special investigations which have been initiated by the BaFin and other supervisory authorities. He has extensive experience in detecting financial crime. He is also part of the global PwC anti-financial crime leadership team and is the sanctions leader of PwC Germany.

PwC

Q. Could you provide an insight into recent trends shaping financial crime in Germany? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Germany is a stable country with a strong internationally interconnected financial centre and, until the COVID-19 crisis, a prospering economy. The country is highly attractive for investments of any kind, including, unfortunately, illicit funds. At the same time, German society is still relatively cash-savvy. Due to the high cash intensity of the economic cycle and the country's economic complexity, overall the money laundering threat to German companies is medium to high. Today, financial crime occurs more frequently and with increased complexity. According to the German national risk analysis, the frequency of money laundering offences in Germany is increasing and the amounts involved are estimated to be more than €100bn annually. The level of fraudulent activity in the German economy has become clearer throughout the COVID-19 crisis. Criminals have recognised and exploited the urge among companies for financial stability, quick claim settlements and governmental economic aid. The deviation from regular processes and routine controls caused by the pandemic has created opportunities for criminals.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Organisations continue to face the threat of money laundering, fraud and terrorist financing, as well as bribery, corruption and sanction violations. We have also seen an increase in cyber crime, often involving the conversion of assets into cryptocurrencies. Suspicious money laundering behaviour can also be detected in the digital sector in Germany, although not yet on a large scale compared to the amounts of money laundered through traditional methods. But cryptocurrencies or virtual currencies are increasingly used to disguise sources of funds. Carelessness or negligence are the most typical sources of financial crime for companies, closely followed by a lack of adequate compliance controls and tools, as well as a lack of awareness of wrongdoing. Regarding

PwC

Companies must take meaningful and timely action as digital solutions, coupled with extensive risk experience, can increase the efficiency of the entire compliance unit and have a significant preventive effect.

compliance tools, many companies have underinvested in compliance digitalisation.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Germany? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Germany has set up national defence mechanisms and regulatory initiatives to combat financial crime activities and we do not believe these to be deficient. Regulatory legislation, such as the Anti-Money Laundering Act, the controlling institution – the Federal Financial Supervisory Authority (BaFin) – and a central office which is supposed to evaluate suspicious cases – the Financial Intelligence Unit (FIU) – are in place to prevent financial crime in Germany. Thus, companies, particularly in the financial services industry, are obliged to follow significant compliance protocols. However, many critics are still calling for improvements to be made in the fight against financial crime, especially regarding the practical implementation of

PwC

legislation, which is currently perceived to be lacking in effectiveness.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: The fight against money laundering, terrorist financing and other criminal offences not only leads to increasing regulatory requirements for companies, as the new Anti-Money Laundering Act in Germany shows, but has also piqued the interest of the public. Due to various recent scandals, such as money laundering via Baltic and Scandinavian banks, supervisory and management bodies see themselves increasingly obliged to defend the integrity and reputation of their organisations in public. Countless government investigations, indictments, judgements and settlements have been, and continue to be, reported in the press on an almost daily basis. The morals and decency of global industries are being questioned by the public. Consequently, supervisory bodies, executives and employees, irrespective of their legal responsibility, should vigorously pursue and promote the establishment of safeguards as part of a new sustainable compliance model and proactively review and revise them if necessary.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Extensive risk experience, entrepreneurial thinking and strategic vision are the basis of a successful compliance programme. The trend of digitalising compliance processes builds on this foundation and has become increasingly prevalent in recent years. Increased technological adoption has many advantages, including increasing efficiency levels, strengthening the prevention of financial crime, being able to make data-driven decisions and helping reduce costs. Digitalisation is already positively impacting organisations. Digital solutions for third-party due diligence, know your customer (KYC) processes, transaction monitoring systems including robotics and artificial intelligence (AI), whistleblowing and case management systems, as well as digitalising compliance reporting and contract management tools, all increase

PwC

companies' ability to detect fraudulent schemes and networks of potential financial crime activity.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: One of the most important considerations for a company which suspects or confirms it has fallen victim to financial crime concerns self-reporting obligations. In terms of money laundering, for instance, the affected company is obliged to immediately investigate the case. Furthermore, it must submit a suspicious activity report (SAR) to the Financial Intelligence Unit (FIU) regardless of the value of the asset involved or the amount of the transaction as soon as indications arise that assets could have been derived from a criminal act or have an illegal origin. It might also be expedient to involve external counsel or consulting expertise to determine the nature and scope of the incident.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: Financial crimes continue to occur at record levels, affecting more companies in a variety of ways. Financial crime is characterised by complex interconnectivity and is not defined by geography, industry or type of organisation. There is a growing need to secure companies against elaborate financial crimes. Given the growing threat posed by financial criminals, and the increasing damage these crimes cause, companies must put effective measures in place to combat financial crime, as well as to test their responsiveness and ability to respond effectively in a crisis. Digital solutions do not have to be expensive and the time to tailor new innovations to case management systems has come. Solutions, such as digital signatures or digital customer on-boarding, process automation and AI, can achieve positive results in compliance at relatively low cost. Companies must take meaningful and timely action as digital solutions, coupled with extensive risk experience, can increase the efficiency of the entire

PwC

compliance unit and have a significant preventive effect.❑

www.pwc.de

PWC advises groups and family-owned companies, industrial and service companies, global players and local heroes, the public sector, associations and NGOs. PwC is the leading auditing and consultancy company in Germany. With more than 12,000 specialists including around 600 partners at 21 locations in Germany, the firm works every day to ensure that this trust is justified.

LARS-HEIKO KRUSE Partner
+49 302 636 2006
lars-heiko.kruse@pwc.com

AUSTRIA

PwC Austria

Respondents

KRISTOF WABL
Partner
PwC Austria
+43 699 1630 5427
kristof.wabl@pwc.com

Kristof Wabl is a partner with PwC Austria, where he leads the forensics & crisis practice. He joined PwC in 2007 and re-entered the Austrian firm after being on secondment in New York from 2011 to 2014. He helps companies prepare for, respond to, and emerge stronger from unplanned events. During his 13-plus years with PwC, he has managed multinational projects across Europe and the US. He has extensive capability in preventing, detecting and investigating fraud, financial crime and other forms of misconduct. Besides PwC, he leads the taskforce whistleblowing team at Transparency International Austria.

CHRISTOPH OBERMAIR
Partner
PwC Austria
+43 699 1087 1262
christoph.obermair@pwc.com

Christoph Obermair is an experienced consulting partner who supports companies in the development of risk, control and monitoring systems. He holds an M.Sc. degree in international economics and business administration from the University of Innsbruck and Trinity College Dublin. Prior to joining PwC, he worked for various consulting boutiques across Europe. He specialises in clients that want to further develop their company-wide risk management. In this context, he advises companies on the revision and optimisation of processes in company-wide risk management.

PwC Austria

Q. Could you provide an insight into recent trends shaping financial crime in Austria? How great a risk does financial crime, such as money laundering, now pose to companies?

A: According to the Austrian Bundeskriminalamt, white-collar crime has been rising steadily for years. In 2019, 71,112 cases, including 43,887 fraud offences, were reported. In terms of money laundering, the Bundeskriminalamt stated that, in 2019, the money laundering reporting office recorded a total of 3656 incoming files, compared to 3494 in 2018. Furthermore, certain types of crime showed a significant increase compared to the previous year: tax offences were up by 155 percent, corruption increased by 121 percent and money laundering saw a 21 percent increase. On the other hand, there was a 38 percent decrease in the number of reports of terrorist financing. Next to the statistical figures, the Austrian banking sector has been hit by insolvency proceedings against a local bank due to alleged fraud in the hundreds of millions over several years.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Organisations continue to be faced with the threat of money laundering, fraud, terrorist financing, as well as bribery and corruption and sanction violations. We see an increase in money laundering in connection with the coronavirus (COVID-19) crisis due to heavy investment into cryptocurrencies, such as Kraken and ETC. In 2020, individuals were defrauded by lucrative offers, through which they were supposed to receive an incoming cash payment, including a substantial commission. Around 33 percent of Austrian companies have been victims of economic crime in the last 24 months, according to our 'Global Economic Crime and Fraud Survey 2020'. The results for Austria show that companies are lagging behind in terms of preventive measures in connection with white-collar crime. More than 25 percent of participants have no fraud risk programmes implemented to address risks related to white-collar crime. Another red flag is that more than half of Austrian

PwC Austria

participants reported conducting only informal risk assessments, or no risk assessment at all, as a preventive measure against white-collar crime.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Austria? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: The legal and regulatory framework in Austria criminalises all forms of white-collar crime. Both money laundering and terrorist financing are criminalised under sections 165 and 278d of the Austrian Criminal Act. Fraud is criminalised under Section 146-148, 150 of the Act. Apart from the regulatory framework, the Austrian Financial Market Authority frequently publishes guidelines for companies and supervised entities to promote best practices in the fight against financial crime. The Bundeskriminalamt not only manages, coordinates and controls all important supra-regional and international crime-fighting measures, but is also the single point of contact for citizens who witness suspicious activities at financial institutions. When money laundering is suspected, companies must report it and file a suspicious activity report (SAR). Another important initiative has been around whistleblowing regulations. All EU member states are obliged to adopt the EU directive on whistleblower protection, which came into force in December 2019 and must be transposed into national law by the end of 2021. The directive is deemed a success in terms of standardising protections for individuals who want to report misconduct. All financial institutions must adhere to the regulation, as well as all companies with more than 50 employees.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Recently, public pressure on financial institutions in terms of anti-money laundering (AML) has increased due to various data leakages and increased regulation. Therefore, financial institutions should adjust to this new battleground – and do so quickly. This includes making sure that both employees and customers are well-informed of emerging and

PwC Austria

evolving threats, implementing cyber and access controls for an increasingly remote workforce, and tuning payment controls needed to help prevent and detect unauthorised disbursements of funds. In addition to shoring up existing controls, the current crisis provides financial institutions with opportunities to rethink traditional fraud management approaches and innovate new ways to help protect their customers. This is also recommended by the Austrian Financial Market Authority, as well as by national and European law.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Like any other business sector, financial crime is becoming increasingly digitalised. In a highly interconnected economic environment that spans multiple jurisdictions, a breach of a single node in the system can affect an organisation's digital landscape in a variety of ways. Therefore, the targeted use of appropriate methods and tools, such as risk rating engines, know your customer (KYC)

The current crisis provides financial institutions with opportunities to rethink traditional fraud management approaches and innovate new ways to help protect their customers.

PwC Austria

processes, case management systems, third-party due diligence, as well as transaction monitoring processes, and the continuous analysis of data, could provide companies with advantages and additional insights in the fight against financial crime. Financial institutions in Austria are starting to use new technologies and data-driven approaches to improve their transaction monitoring systems to identify anomalies and to implement a more efficient, targeted approach. This is a milestone, as AML is increasingly complex and, due to its digital form, harder to identify.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Collect the facts via the key stakeholders involved, such as legal, human resources, IT and management. Immediate actions should also include consulting with local regulators and checking self-reporting obligations, such as a SAR. It may be useful to involve independent consultants to mitigate risks and fully investigate the case.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: For most companies, it is a huge challenge to tailor new innovations to the operational life of a business. Budget and staff constraints, management prejudice in terms of efficiencies, deviation of the daily routine or lack of know-how are only some points to mention. To improve the way they manage financial crime risk, companies must ensure that customer due diligence rule requirements are implemented seamlessly across the entire global organisation. Leadership should create and support a culture of compliance and focus on the organisation's anti-financial crime efforts. Companies should also stay up-to-date with fraud crimes, new rules and new technologies. Assessing risks is not only important within an organisation but also with third-party relationships. Finally, having sophisticated data-driven and analytically capable platforms helps organisations to develop.❑

PwC Austria

www.pwc.at

PWC's purpose is to build trust in society and solve important problems. PwC is a network of member firms in 157 countries, with more than 276,000 people around the world providing high-quality services across the areas of audit, tax and legal services, and advisory work. PwC Austria has offices in five different locations and has around 1200 employees and 60 partners. The public sector, banking institutions, as well as local and global leading companies – from family run businesses through to global corporations – have all come to appreciate the firm's expertise.

KRISTOF WABL Partner
+43 699 1630 5427
kristof.wabl@pwc.com

CHRISTOPH OBERMAIR Partner
+43 699 1087 1262
christoph.obermair@pwc.com

MALTA

FTI Consulting

Respondents

MILES HARRISON
Consultant
FTI Consulting
+44 (0)20 3727 1163
miles.harrison@fticonsulting.com

Miles Harrison is a consultant in the financial services practice at FTI Consulting, where he advises a range of governments and financial institutions on complex regulatory, operational and financial crime concerns globally. In Malta, he has worked extensively with the regulatory and enforcement community to investigate suspicious activity and optimise financial crime supervision, with a focus on preventing money laundering, corruption, terrorist financing and sanctions evasion, as well as governance and prudential weaknesses.

FEDERICA TACCOGNA
Senior Managing Director
FTI Consulting
+44 (0)20 3727 1000
federica.taccogna@fticonsulting.com

Federica Taccogna is a senior managing director in the financial services team within the financial and litigation consulting segment at FTI Consulting. She is based in London. Having previously held senior risk and compliance positions in industry, including head of controls, head of operational risk and head of compliance, Ms Taccogna now supports a broad range of financial services institutions and regulators globally advising on, investigating and remediating regulatory and financial crime, in particular money laundering and terrorist financing, and governance and control concerns.

FTI Consulting

Q. Could you provide an insight into recent trends shaping financial crime in Malta? How great a risk does financial crime, such as money laundering, now pose to companies?

A: It is no secret that Malta's rise as a financial centre has faced headwinds in recent years due to financial crime concerns that have exploited the jurisdiction's favourable business climate. In response, authorities have prioritised improving the jurisdiction's understanding of the problem, including by issuing new guidance and conducting more investigations. Although trending toward a more sophisticated understanding means that regulators and firms have a stronger chance of identifying money laundering and other illicit typologies, it does not necessarily lead to a reduction in criminal activity. Much like other jurisdictions, financial crime continues to evolve in volume and complexity, particularly in areas known to present a higher degree of risk, such as banking, corporate service providers, cryptocurrencies – the island awarded its first virtual assets licence in November 2020 – e-money, gaming firms and payment service providers. In recognising the true scale and interconnected nature of the prudential and financial crime risks facing the jurisdiction, though, Malta has begun to pursue more aggressive enforcement action.

Q. In your experience, what are the main types of financial crime that organisations encounter? What are the typical sources of such risks?

A: Malta's geographic location and economic and cultural ties to Europe, Africa, the Middle East and Asia present a unique set of opportunities, including for financial crime. As a result, Malta-based firms encounter a wide spectrum of illicit activity, ranging from foreign organised crime involved in bribery, corruption, fraud and money laundering to high-risk, high-net-worth individuals who seek to take advantage of Malta's tax environment and citizenship-by-investment scheme, some of whom have adverse media and, in some cases, a criminal record. Malta's institutions are often exposed to a high ratio of non-resident customers and large volumes of transactions facilitated by payment service providers and prepaid

FTI Consulting

card providers, thereby creating a more fertile end-to-end environment for money laundering. The jurisdiction's large shipping sector also raises the level of sanctions-related risk, particularly when it comes to Russia, Libya and the Middle East.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Malta? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Malta is constantly improving its legal and regulatory framework to combat financial crime. The Malta Financial Services Authority (MFSA), in tandem with the Financial Intelligence Analysis Unit (FIAU), are set to expand the scope of their routine visits and investigations, leading to an increase in enforcement action for violations of the Implementing Procedures (IPs), Prevention of Money Laundering Act (PMLA) and Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). Importantly, the FIAU has continued to improve the IPs based on the identification of new typologies and by engaging the private sector. Collectively, these actions mean that the demands on firms are greater, but also clearer. Nevertheless, some firms in Malta struggle to implement the procedures in practice due to the fact that the market for compliance resources is expensive and requires skills that are not readily available locally. At the European level, we also note a number of developments that are set to affect the legal and regulatory landscape in Malta. From June 2021, the 6th Anti-Money Laundering Directive will come into effect, harmonising the list of predicate offences, expanding the definition of money laundering, introducing criminal liability for legal persons and improving information-sharing channels.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Companies should proactively improve their compliance programmes before the regulator is even at their doorstep – saving them time, cost and reputational damage. If, however, a firm is subject to enforcement action, as in the case of

FTI Consulting

several recent examples taken by the MFSA and the FIAU, it may be mandated to conduct a remediation exercise to improve its financial crime controls – that is, if it is not shut down entirely. More sophisticated firms understand that enforcement actions brought by regulators also offer a window of opportunity to proactively assess and improve their financial crime compliance frameworks. These operators recognise that financial crime is an evolving threat – criminals are constantly looking to exploit weaknesses in the entire system – and that it is essential to conduct rigorous testing to evaluate the effectiveness of their compliance programmes.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: There is no doubt that technology is vital in fighting financial crime, but it is also a double-edged sword. As elsewhere, we have seen criminals deliberately exploit technology to forge documents, disaggregate customer data by placing servers in jurisdictions with weak data

There is no doubt that technology is vital in fighting financial crime, but it is also a double-edged sword.

FTI Consulting

governance laws, and wash billions of euros through complex money laundering schemes using cryptocurrencies and the dark web. At the same time, Malta's investigators, regulators and firms are moving from having fairly simple systems in place to adopting increasingly sophisticated technologies, including artificial intelligence and machine learning, to automate certain screening and transaction monitoring processes. The role of technology should also not be overestimated: this narrative benefits the technology providers that claim to offer one-size-fits-all, silver-bullet solutions. Although techniques such as network analysis and advanced risk-rating models can be helpful from a cost and depth perspective – for instance, identifying anomalies not seen by the naked eye, or reducing the quantity of false positive results – they ultimately serve to complement, not replace, human expertise.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Malta is in line with the trends that we see in other jurisdictions. Financial institutions and, increasingly, non-financial firms are investing significant sums of money into compliance to meet regulatory expectations to promptly identify and report suspicious activity. What money alone fails to address, however, is the process of taking stock of how financial crime exploited the institution in the first place, ensuring that failures are remediated and preventing issues from reoccurring. In other words, reporting is only one facet of the response. Instead, it needs to be complemented by exercises such as lookback reviews, continuous staff training, and improvements to processes, procedures and controls. Awareness of the problem has increased and, as a result, firms are taking the initial step to report financial crime – the FIAU has experienced a roughly 400 percent increase in the number of suspicious transaction reports (STRs) submitted over the past four years.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

FTI Consulting

A: Our advice to firms in Malta and elsewhere is simple. First, understand the financial crime risks to which you are exposed. This requires constant reflection and evaluation of the risk vectors, as well as appropriate allocation of resources. Second, mitigate the risks identified by designing and evaluating a framework of controls that enable your firm to internalise the letter and spirit of regulation – too often, we have inspected firms in Malta and elsewhere that skipped the ongoing self-evaluation step and viewed their 'controls' as a one-time, tick-box exercise. Third, ensure your staff are trained appropriately, across the three lines of defence. Although technology and expertise is available to assist with financial crime compliance, including ongoing monitoring and payment screening, firms with advanced systems may still fail to pass regulatory assessments if staff are unaware of the risks faced.❑

www.fticonsulting.com

FTI CONSULTING is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. Individually, each practice is a leader in its specific field, staffed with experts recognised for the depth of their knowledge and a track record of making an impact. Collectively, FTI Consulting offers a comprehensive suite of services designed to assist clients across the business cycle.

MILES HARRISON Consultant
+44 (0)20 3727 1163
miles.harrison@fticonsulting.com

FEDERICA TACCOGNA Senior Managing Director
+44 (0)20 3727 1000
federica.taccogna@fticonsulting.com

ROMANIA

KPMG Romania

Respondents

ANGELA MANOLACHE
Advisory Partner
KPMG Romania
+40 740 100 649
amanolache@kpmg.com

Angela Manolache is a financial services advisory partner for KPMG in Romania and leads the network of financial risk management professionals for KPMG in Central and Eastern Europe. With over 20 years of experience in professional services, she has assisted numerous financial institutions in the local and regional market in enhancing and aligning their internal risk and compliance frameworks to the latest regulatory developments and to international best practices. She also collaborates on a regular basis with regulatory bodies and professional associations on projects and initiatives supporting local regulatory reform.

CALINA IACOB
Advisory Director
KPMG Romania
+40 751 222 757
ciacob@kpmg.com

Calina Iacob leads the risk and compliance practice area for KPMG in Romania and has extensive experience working with financial institutions in strengthening their risk management, corporate governance and compliance frameworks. She is a specialist in regulatory change and transformation and has been advising banks on enhancing their KYC, AML and CTF policies, procedures, processes and systems in light of the ever increasing requirements in this area. She is a certified public accountant and financial risk manager and a member of the local audit and accounting professional bodies.

KPMG Romania

Q. Could you provide an insight into recent trends shaping financial crime in Romania? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Despite recent progress made in upgrading its legal framework and intensifying monitoring and enforcement actions against financial crime, Romania remains particularly vulnerable to money laundering and terrorism financing activities given its peripheral position within the EU, as well as its specific economic and institutional weaknesses. Romania was known as a hub for cyber crime long before the COVID-19 pandemic, with both the volume and sophistication of attacks continuing to grow despite significant coordinated national and international efforts aimed at curbing the phenomenon. These threats have been accentuated by the COVID-19 crisis, which has increased both economic vulnerability and exposure to cyber risk for individuals and companies, given restrictions on activities posed by social distancing rules and an accelerated shift toward the internet and remote working. Once finalised, the first nationwide money laundering/counter terrorism financing (ML/CTF) risk assessment, currently ongoing with assistance from the Council of Europe under the EU 2020 Structural Reform Support Programme, is expected to bring more insight into Romania's specific threats and vulnerabilities to financial crime and allow more targeted efforts.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Given Romania's inherent vulnerabilities to financial crime, as well as the general lack of awareness in the field, individuals and organisations continue to be exposed to some of the more obvious financial crime schemes, such as chief executive fraud, invoice fraud, phishing and personal data theft, among others. More elaborate schemes have recently been uncovered due to collaborative efforts from national and international authorities, demonstrating the benefits of cross-border collaboration. On a national level, both supervisory authorities and banks have stepped up

KPMG Romania

With every passing second new data is being generated and new information on customer identity and customer behaviour is becoming available, which cannot be ignored by FIs or other reporting companies.

their efforts to improve awareness of financial crime risk among companies, employees and the general population via targeted communications and educational campaigns. However, there is still much to be done by both companies and financial institutions (FIs) in terms of adapting their internal frameworks to the new laws and regulations, strengthening internal controls and expanding available resources and expertise to effectively fight both traditional and more innovative types of financial crime.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Romania? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Romania has stepped up efforts to align its internal framework with the latest European developments. In July 2020, new amendments to the local AML legislation were adopted also in line with the 5th EU AML Directive, introducing new requirements in terms of ultimate beneficial owner (UBO) identification, know you customer (KYC)

and reporting obligations, and extending the list of entities obliged to monitor and report suspicious transactions to new categories of market players, such as real estate developers but also virtual wallet and cryptocurrency service providers. Enhancement of the local AML/CTF framework is due to continue as the European Commission intensifies its push for a harmonised and coordinated effort against financial crime at the EU level, while supervisory authorities are boosting their ranks in an effort to keep up with both the threats and demands of an ever-evolving regulatory framework.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Enforcement of the updated regulatory framework against financial crime puts pressure on FIs, which must ensure that their procedures, when accepting new clients or providing services, are adequately structured to reduce their risk of being used as vehicles of financial crime. Nevertheless, their efforts will likely never be enough, as incidents such as chief executive fraud or invoice fraud take place primarily due to weaknesses at the level of the company, not only at the level of FIs. Hence, it is very important that companies and individuals proactively seek to ensure that the way they perform their activities protects them against financial crime, and collaborate with FIs in their actions to identify money laundering or other types of financial crime.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Despite Romania's historically low levels of digitalisation and reduced penetration of even the more traditional forms of financial services, the shift to online processes, such as opening accounts with FIs, registration with or reporting to public authorities or national registries, has greatly accelerated during the COVID-19 era. As a result, with every passing second new data is being generated and new information on customer identity and customer behaviour is becoming available, which cannot be ignored by FIs or other reporting companies. Hence, there is a need for

greater information processing capacity and sharper instruments to identify financial crime quickly and efficiently. On the other hand, the rise of FinTech, including virtual currencies, has opened a new door for financial criminals, thus organisations must be agile enough to swiftly adapt to new threats. Tools such as machine learning and artificial intelligence have a key role to play in this fight.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: Generally, the first thing a company should do is to try to find a way to 'stop the bleeding', and in this respect the most immediate action would be to contact the relevant parties, such as management, banks, IT experts and so on, to take any immediate action required, such as blocking a transaction or payment instrument, securing the data, the IT systems and so on. The next step would be to report the incident to the relevant national authorities, both to get their support and for the initiation of the required investigations. For example, in Romania CERT.RO is the competent national authority for IT networks and systems, and the Computer Security Incident Response Team (CSIRT) is the national contact in case of cyber crime incidents. Nevertheless, if we think about a typical small and medium-sized enterprise (SME) operating in Romania, the company should have clear risk-mitigating actions, such as specific procedures for higher risk processes, including online payments, in place and predefined contingency plans and escalation rules, given that typically in the case of a financial crime incident time is of the essence and employees should already know what steps to take and who to contact and thus be able to act swiftly.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: The most important step is to stay informed on the potential threats posed by financial criminals which are typical for Romania, using official and credible sources of information. For example, CERT.RO publishes recommendations

KPMG Romania

for companies and their employees on remote working in secured conditions, and on how to avoid the most frequent fraud schemes, while other established companies which specialise in AML or cyber security assistance regularly publish newsletters or articles on these topics. Secondly, companies should perform a risk assessment of their activity and ensure that mitigating actions are taken, such as instituting clear rules for how and when to make electronic payments, defining clear roles and competences in relation to the company's assets, training relevant staff, conducting expert cyber security reviews and so on. Thirdly, companies should have contingency plans for different types of threats – who does what following an incident, who needs to be contacted and so on.❑

www.kpmg.com

KPMG operates as a global network of independent member firms offering audit, tax and advisory services; working closely with clients, helping them to mitigate risks and grasp opportunities. Member firms' clients include business corporations, governments and public sector agencies and not-for-profit organisations. They look to KPMG for a consistent standard of service based on high order professional capabilities, industry insight and local knowledge.

ANGELA MANOLACHE Advisory Partner
+40 740 100 649
amanolache@kpmg.com

CALINA IACOB Advisory Director
+40 751 222 757
ciacob@kpmg.com

AUSTRALIA

Ernst & Young Australia

Respondents

SCOTT MANDELL
Partner
Ernst & Young Australia
+61 (2) 9694 5696
scott.mandell@au.ey.com

Scott Mandell is a co-leader of EY financial crime advisory services for the Oceania market. With 20 years of experience in fraud detection and anti-money laundering (AML) compliance, he led engagements for some of the largest global financial institutions ranging from peer benchmarking, policy, procedure reviews and assessments, as well as regulatory lookbacks and remediation efforts. He also spent time with front and back office functions, risk and compliance groups, data management, governance offices and worked extensively with the technology counterparts of each.

MIKE ALLEN
Associate Partner
Ernst & Young Australia
T: +61 (2) 8295 6193
E: mike.allen@au.ey.com

Mike Allen is an associate partner and co-lead of EY Oceania financial crimes services. He formerly led a financial crime operations team of over 1100 people at a major Australian bank. Possessing a broad range of subject matter knowledge and expertise, he applies more than 20 years of hands-on financial services experience to conduct business investigations and reviews on behalf of clients who seek to improve their financial crime ecosystem. With a background in process optimisation, emerging technology and delivery, he is able to simultaneously solve customer, organisation value and regulatory challenges across the customer lifecycle.

Ernst & Young Australia

Q. Could you provide an insight into recent trends shaping financial crime in Australia? How great a risk does financial crime, such as money laundering, now pose to companies?

A: In September 2020, the Australian Transaction Reports and Analysis Centre (AUSTRAC) issued a record high AU$1.3bn anti-money laundering (AML) fine to an Australian financial institution, the largest such fine in Australia's corporate history – surpassing the previous highest penalty amount, from 2018, by AU$500m. Unsurprisingly, the threat of large financial penalties, combined with a significant increase in regulatory scrutiny, has led to a greater focus from boards on managing financial crime risks. Over the last year, the coronavirus (COVID-19) crisis has also changed customer behaviour, with a large contingent of the population working from home, and limitations on local and international movement. This has led to rapid growth in areas such as online shopping, and it has become more challenging to define what an unusual transaction is against this backdrop of evolving consumer behaviour.

Q. In what ways does globalisation impact local institutions' ability to manage financial crime?

A: Historically, Australia has had a very heavy focus on the domestic market which, to a large extent, shielded us from some of the worst financial crime activity. As we become increasingly more globalised though, we are exposed to a similarly increasing complexity of international financial crime risks and activities. Many Australian organisations' existing risk structures and controls are not fit for this heightened exposure, and there is a need to uplift capability in this space to reflect global best practices. For example, investment is required to help financial institutions focus on customer and payment screening for sanctioned parties to a higher standard. One benefit of Australia's relative latency is that we can leverage the lessons learned by other, more experienced jurisdictions, providing us the benefit of a steeper maturity curve. Adopted well, these learnings could provide an opportunity for Australian organisations to accelerate to global best practice faster than we have observed internationally.

Ernst & Young Australia

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Australia? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: Beyond the threat of hefty fines, a broader market increase in regulatory action and engagement is apparent right across the Australian financial services industry. Broad risk cultural shortcomings often include weaknesses in the AML environment and a historical unwillingness to invest in modern systems and practices for functions previously considered a cost centre. As organisations grapple to rapidly improve their risk and control environment, they are also faced with a baseline which was implemented over a decade ago and still requires them to address many longstanding issues. As a result, a significant backlog of issues requiring remediation needs to occur in parallel with new activities designed to uplift and improve current systems and processes. This heavy workload places a significant strain on a very limited talent pool of financial crime resources in the Australian marketplace.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

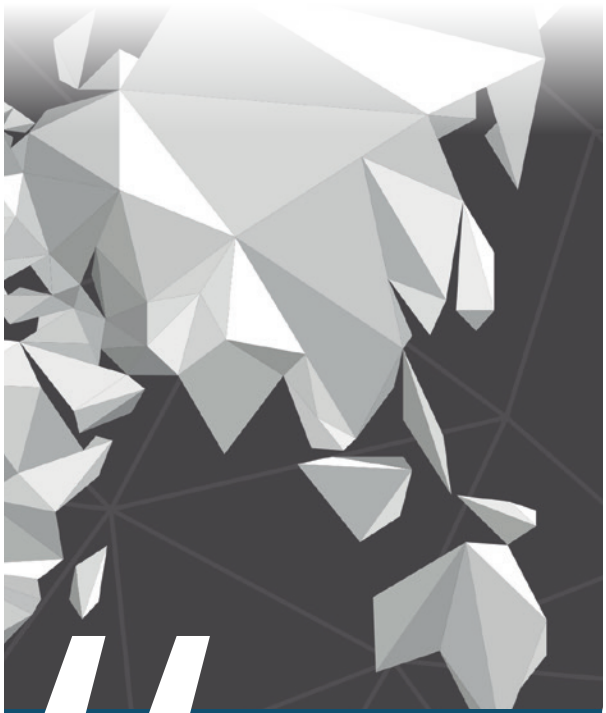
A: The policies and practices in place across many organisations in Australia today have only had incremental changes made to them since the introduction of AML legislation in 2006. The expectation of AUSTRAC is that increases in AML procedures will remain effective at fighting the latest global movements in financial crime. So, the desire is to not just reach parity with current expectations and standards, but to be on the front foot against ever-increasing and evolving risks. As a result, the Australian market is both catching up and striving to achieve the next level of security over a very short time period. Recently, a number of organisations have invested heavily to improve their AML capabilities, as a result of enforcement actions. This creates momentum for others to follow. Companies that were previously seen as domestic AML leaders risk falling behind unless they dedicate a similar focus to remaining current with their risk controls and systems. In addition, deep regulatory engagement is required at all levels of

Ernst & Young Australia

the organisation, from the board down. Proactive, forthright and transparent engagement with the regulators are increasingly the norm, providing transparency around both known deficiencies and improvement strategies.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Technology is a crucial enabler in the fight against financial crime. Increasingly, modern technologies such as artificial intelligence can help reduce cost bases while increasing auditability and traceability. New technologies can also provide more consistent and sophisticated identification methods for unusual patterns, and assist with investigations processes, such as more complete entity resolution. Best practice financial crime management is also becoming increasingly real-time, which requires the use of modern technology. Real-time capability improves customer and user experience – enabling immediacy around meeting client and staff needs to obtain services required, while simultaneously preventing financial



Proactive, forthright and transparent engagement with the regulators are increasingly the norm, providing transparency around both known deficiencies and improvement strategies.

Ernst & Young Australia

crime. Further organisational value is delivered through a significantly more efficient process.

Q. How are companies operationalising the management of financial crime?

A: A strong financial crime cultural awareness drive is underway to obtain greater buy-in across organisations, with a particular focus on the human impact. Change management programmes are being put in place to ensure policies are operationalised across risk, technology, operations and the wider business. Typically sponsored by the chief risk officer (CRO), a strong programme leader will work with financial crime policy and operations teams and be supported with business representation to ensure policies are implemented in a customer-focused and efficient way. Organisations are often challenged to apply top-down messaging around zero financial crime risk tolerance when setting product features, such as cash-based deposit limits. Policy and disposition 'greyness' requires an element of risk-based decision making to determine the best way forward and ensure the desired risk appetite level is achieved. This greater focus on driving more stringent financial crime policy, larger rules volume and high levels of change activity in tandem is in turn leading to significant increases in resourcing requirements across the industry.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: While a clear catalyst for improvement is evident, any financial crime uplift activities still need to compete for scarce investment funding with an increasing range of other regulatory and growth initiatives. As such, a real opportunity exists to understand how convergence between risk management, improved customer experience and growth can be achieved in tandem, through designing solutions with a customer lens.❑

Ernst & Young Australia

www.ey.com

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets. Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate. Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

SCOTT MANDELL Partner
+61 (2) 9694 5696
scott.mandell@au.ey.com

MIKE ALLEN Associate Partner
+61 (2) 8295 6193
mike.allen@au.ey.com

EY Building a better working world

ISRAEL

PwC Israel

Respondent

ERAN RAZ
Partner
PwC Israel
+972 54 666 02 60
eran.raz@pwc.com

Eran Raz leads the risk and forensic practice for PwC in Israel. He has more than 16 years' experience leading strategic and tactical projects in the department, for which he provides in-depth advisory support to institutions varying in size, industry and complexity, both in Israel and globally. He has extensive experience leading engagements on issues related to regulatory compliance, internal and external fraud (fraud risk identification and management), financial crimes, investigations, forensic accounting matters, anti-corruption, BSA/AML compliance, corporate intelligence and forensic technology services in order to help local and global companies to mitigate risk, address regulatory issues and uphold obligations

PwC Israel

Q. Could you provide an insight into recent trends shaping financial crime in Israel? How great a risk does financial crime, such as money laundering, now pose to companies?

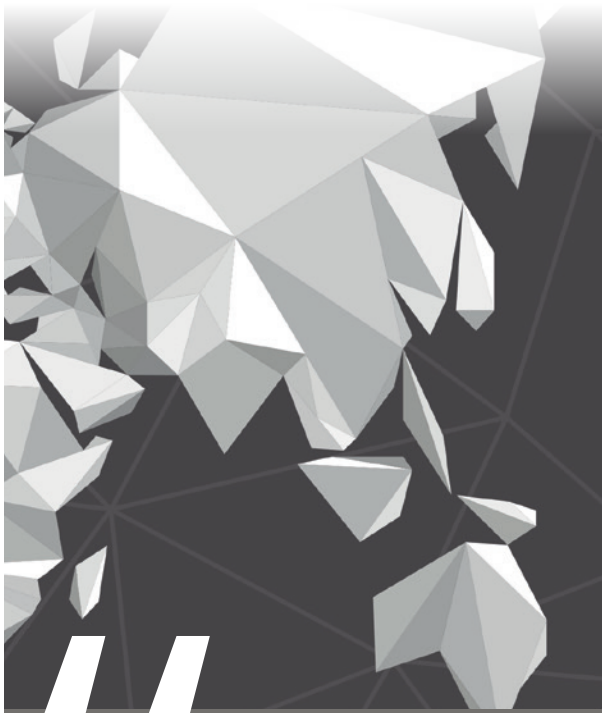
A: Since the onset of the COVID-19 crisis, we have seen an increase in the three main types of financial crimes in Israel – customer and employee fraud and cyber crime. These, together with bribery and corruption risks, were ever present throughout 2020 and they had a significant impact on the business landscape. Businesses are now increasingly allocating more resources to fighting and managing financial risks. Anti-money laundering (AML) efforts are receiving significant attention given the current market conditions. Many companies are adopting a positive and proactive approach to addressing their AML challenges by implementing internal controls and procedures to manage the risk and the exposures. This behaviour is directly derived from the strict supervision of Israel's AML regulator.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: The three most prominent forms of financial crime that organisations are encountering – customer fraud, employee fraud and cyber attacks – are related to the fact that 2020 was an anomalous year due to COVID-19. Remote working has created many opportunities for organisations, as well as various challenges. Those organisations which lacked a proper security framework were exposed to cyber attacks and data leakage. Furthermore, the layoffs and furloughs experienced in many businesses have revealed gaps in internal control frameworks, which have created opportunities for internal frauds, particularly in procurement processes, payments and cash management. Finally, we saw many attempts at social engineering and phishing attacks on organisations, leading to some significant cases of data and financial theft.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in Israel? How would you describe the nature and extent of the

PwC Israel



Companies should establish an AML framework, appoint a money laundering reporting officer (MLRO), conduct an AML risk assessment and establish an internal and external reporting process.

demands being placed on companies to help reduce financial crime?

A: Know your customer (KYC), screening and AML monitoring and investigations are the key controls to prevent financial institutions from falling victim to financial crime. Despite the evolution of regulations governing these practices over the past decade, their effectiveness and efficiency often remain an issue. While some individuals and organisations have moved to digital and interconnected solutions, many companies are still relying on outdated security measures. Due to the COVID-19 crisis, companies will continue to be exposed to financial crime risk.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Companies in Israel should proactively review and revise their practices, especially in terms of AML measures and ensure the existence of an appropriate supporting organisational infrastructure. Companies should establish an AML framework, appoint a money laundering reporting officer (MLRO), conduct an AML risk

PwC Israel

assessment and establish an internal and external reporting process. In addition, ongoing monitoring processes should be implemented as part of the in-place control framework. In accordance with supplement three of the Israeli Prohibition on Money Laundering Laws, the entities to which the law applies, other than banks, are members of the stock exchange, portfolio managers, insurers and insurance agents, management companies, regarding the provident funds under their management, currency exchange providers and postal banks. These entities are required to appoint an MLRO. In accordance with Ministry of Justice-issued regulation published in May 2020, a financial and business entity is required to identify the risks of money laundering and terrorist financing to which it is, or will be, exposed, and to establish a risk assessment according to which a risk-based approach will be implemented.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: Technology receives significant attention in the current Israeli business environment, particularly with regard to fighting financial crime. This increase starts with the regulators who encourage institutions to digitalise their controls frameworks, together with enhancing on-boarding processes by utilising enhanced due diligence technologies. Second, organisations are increasingly applying big data tools to their internal available data for generating insights and identifying potential trends or anomalies with regard to financial crime and risks. Finally, there has been an increased demand for the use of automation, usually integrated into the on-boarding, payment and receivables phases.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: There are several essential steps which must be taken, which are also backed by financial regulation that guides instructions on how to deal with identified financial crime. First, report the incident to senior management and notify the board of directors regarding the suspected event.

PwC Israel

Then, appoint a team to manage the event and report to the board and management regarding the investigation. It is highly recommended that the team be granted the necessary authorisation to conduct the investigation. Furthermore, companies should hire independent investigators who can quantify the potential damage, identify the roots and the causes of the event and map the involved entities. Investigators should work closely with the internally appointed entity regarding the investigation. Once a clear understanding of the breach is obtained, the company must report the event via the relevant channels.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: Companies must understand that financial crime management is crucial. Companies must use the various tools and techniques at their disposal to address these risks, including financial crime risk assessments, which will help to map and understand the overall risk landscape the company faces. Furthermore, based on the identified risks and exposure, companies should consider implementing controls and process, which will help mitigate the risk. Companies across industries can successfully incorporate new technological innovations and put in place a strategy and commit to making a specific set of moves to improve their financial crime risk management.❑

PwC Israel

www.pwc.com

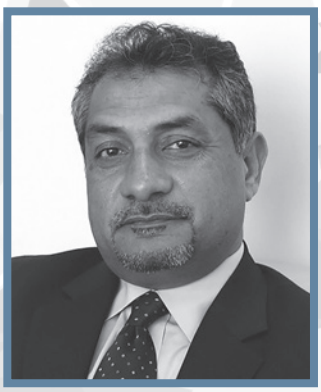
PWC ISRAEL is a leading professional services firm in the Israeli market. Established in 1924, the firm currently has about 61 partners and over 1000 professionals, including accountants, economists, attorneys, MBAs, programmers, data analysts, engineers and more. As is the common practice in the global network, the firm's services are classified into three main lines, accounting, tax and advisory, each with its unique expertise and tools to address the needs and requirements of clients operating in both local and global markets.

ERAN RAZ Partner
+972 54 666 02 60
eran.raz@pwc.com

UNITED ARAB EMIRATES

Corporate Research and Investigations Limited

Respondents



ZAFAR ANJUM
Group Chief Executive Officer
Corporate Research and Investigations Limited
+44 (0)7588 454959
zanjum@crigroup.com

Zafar Anjum is founder and group CEO at CRI Group, and its ABAC Center of Excellence. He uses his extensive knowledge and expertise in creating stable and secure networks across challenging global markets. For organisations needing large project management, security, safeguard and real-time compliance applications, Mr Anjum is the assurance expert of choice for industry professionals.

HUMA KHALID
Scheme Manager
ABAC Center of Excellence Limited
+44 (0)777 652 4355
huma.k@abacgroup.com

Huma Khalid, as scheme manager, is responsible for leading ABAC. Ms Khalid's responsibilities include planning and overseeing all aspects of the ABAC programme, which include certification and training. Additionally, she oversees the compliance department for the implementation, management and internal audit of CRI Group's and ABAC compliance programmes.

Corporate Research and Investigations Limited

Q. Could you provide an insight into recent trends shaping financial crime in the UAE? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Fraud and financial crime is a worldwide problem, and we are not immune to its impacts in the UAE. The UAE has taken a strong stance against corruption and consistently leads the Middle East in Transparency International's Corruption Perceptions Index for its efforts. The recent Anti-Commercial Fraud Law strengthened protections of intellectual property rights (IPR) and imposed stricter penalties on counterfeiters. However, certain crimes, such as money laundering, are causing increased concern in the region. The flow of illicit funds in Dubai is beginning to cast a shadow for international business conducted in the region and should urgently be addressed. Money laundering has been linked to major crimes and even terrorism, and no company in the UAE wants to be associated with high-level criminal conduct of that nature. That is why it is critical for organisations both public and private to have the highest level of anti-money laundering (AML) controls in place and be fully AML compliant.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: Along with money laundering risks, we are seeing an increase in cyber crime and data theft. Organisations in the UAE are finding cyber security to be an urgent need, as phishing schemes are being rolled out on a larger scale against company workforces to try to exploit vulnerabilities. If a phishing attack targets a large corporation, all it takes is one employee falling for the scheme to potentially expose the entire company and their data. When it comes to money laundering, a recent report from Carnegie Endowment found that there is a steady stream of illicit funds from corruption and crime flowing into the UAE. This should be alarming to organisations and regulators alike. The perpetrators take advantage of 'free trade zones' and often the money is funnelled through real estate deals, especially in luxurious properties in Dubai, for instance. This might be facilitated by foreign

Corporate Research and Investigations Limited

mobsters, gold smugglers, and even warlords. These are high-level criminal operations that can pose a risk to any legitimate organisation operating in the UAE and the Middle East as a whole.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in the UAE? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: At least two laws in the UAE are the foundation for combatting money laundering and terrorist financing: Law No 4/2002, the Anti-Money Laundering law, and Law No. 1/2004, the Counter Terrorism Law. The Anti-Commercial Fraud Law strengthened other areas of combatting financial crime, including counterfeiting and intellectual property theft. The tools are largely in place, and now the issue comes down to enforcement. Fraud is not tolerated, and companies in the UAE face strong punishments for financial crimes. Money laundering, however, still represents a gap in enforcement, and organisations should not wait for government action to put their own AML frameworks in place. Like many countries around the world, the UAE is experiencing an uptick of fraud and financial crimes during the COVID-19 pandemic.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

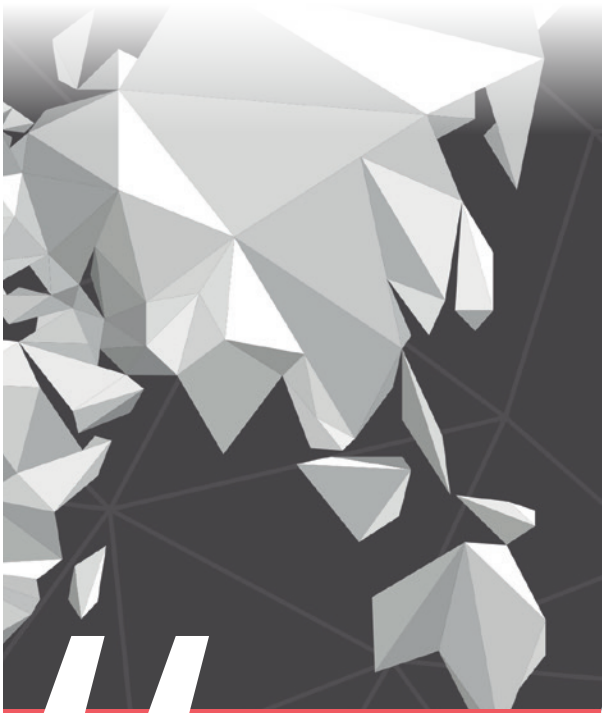
A: Organisations should always be reviewing and revising their business practices with risk management and fraud prevention in mind. Facing enforcement action just means they have likely already waited too long. Unfortunately, sometimes that is what it takes to initiate needed changes. Organisation leaders should sit down with risk management and fraud prevention experts to examine what went wrong, implement proven strategies to prevent future failures, and identify other vulnerabilities that add to the organisation's overall risk profile. Taking action, and communicating that action, demonstrates to regulators and stakeholders a commitment to compliance. Facing enforcement action for compliance failures should kick off a process that includes training, certification

Corporate Research and Investigations Limited

and evaluation at regular intervals. Enforcement action often arises from incidents of bribery and corruption. A training and certification programme for the world-recognised ISO 37001 Anti-Bribery Management Systems standard can set an organisation on the right track to addressing its challenges head-on.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: For years, financial institutions have used technology to help detect and combat money laundering, and organisations should follow their example. The latest technological solutions can automate processes that would take far too long, and expend too many resources, for employees to conduct on their own. New software can quickly analyse billions of data records to spot potential money laundering activity. Artificial intelligence (AI) and machine learning are no longer sci-fi or futuristic concepts: the technology is here. The key is engaging experts, a third-party firm if needed, to tailor the right solutions to your organisation and



The latest technological solutions can automate processes that would take far too long, and expend too many resources, for employees to conduct on their own.

Corporate Research and Investigations Limited

implement them effectively. At a recent AML conference, case studies were presented that showed just how technology can really help ramp up the fight against this type of financial crime. The most successful elements included information sharing, such as a database of bad actors that is made accessible to organisations, and language and text analytics to sift through countless transactions and red flag potential criminal activity. Rolling out an AML strategy at your organisation should include technological solutions combined with employee training for preventing and detecting money laundering.

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: When financial crime is suspected or confirmed, owners or managers need to bring in experts to conduct a proper investigation. To not do so risks mishandling evidence or even violating certain laws, such those dealing with privacy, that can impact the case and company itself. If there is evidence of fraud, law enforcement or regulators should be contacted, and perpetrators prosecuted. Some large corporations have teams of dedicated fraud prevention and detection experts on staff who are trained to handle financial crime cases. Many organisations, however, do not have such personnel on staff. When this is the case, it is imperative to reach out to a fraud investigation firm that is trained to provide expert help. Everything from interviewing witnesses to collecting and analysing evidence may be scrutinised later.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: When organisations implement AML and other fraud prevention solutions, they quickly learn that not only is it very feasible to tailor a programme to their own operations, it is also the only right way to do it. There is no 'one-size-fits-all' solution for compliance and risk management. By implementing best practices and resources that are known to be effective for the organisation's risk profile, leaders can rest easier knowing that they have

Corporate Research and Investigations Limited

the tools in place to prevent and detect financial crime. It is important that business leaders adopt the mindset that risk management and fraud prevention is a core business function, not apart from it. This is underscored by the fact that just one serious case of fraud can seriously damage or even ruin a company, whether through financial harm, reputational harm or both. Companies that are adaptable and forward thinking will embrace the opportunity to integrate risk management processes into their operations. They will likely see other benefits as well, such as increased efficiency, enhanced reputation and more partnering opportunities with other organisations that value ethics and transparency.❑

www.crigroup.com

CRI GROUP works with companies across the Americas, Europe, Africa, Middle East and Asia-Pacific as a one-stop international risk management, employee background screening, business intelligence, due diligence, compliance solutions and other professional investigative research solutions provider. CRI Group has the largest proprietary network of background-screening analysts and investigators across the Middle East and Asia. Its global presence ensures that no matter how international your operations are, the company has the network needed to provide you with all you need, wherever you happen to be.

ZAFAR ANJUM Group Chief Executive Officer
+44 (0)7588 454959
zanjum@crigroup.com

HUMA KHALID Scheme Manager
+44 (0)777 652 4355
huma.k@abacgroup.com

RAZA SHAH Business Development and Marketing Executive
+92 300 501 2632
raza.shah@crigroup.com

AYESHA SYED Lead Auditor
+971 4 358 9884
ayesha.s@abacgroup.com

CRI | GROUP
Corporate Research and Investigations

SOUTH AFRICA

KPMG

Respondent

DÉAN FRIEDMAN

Director
KPMG

Déan Friedman is currently employed by KPMG Forensic's South African practice in the capacity as director, among others responsible for forensic and investigative assignments in the Africa region. He is the investigations leader at forensic in South Africa, overseeing the corporate intelligence service at forensic and responsible for asset preservation services. He commenced his career as a prosecutor and state advocate in the service of the Director of Public Prosecutions, where he was responsible for the prosecution and high level fraud.

KPMG

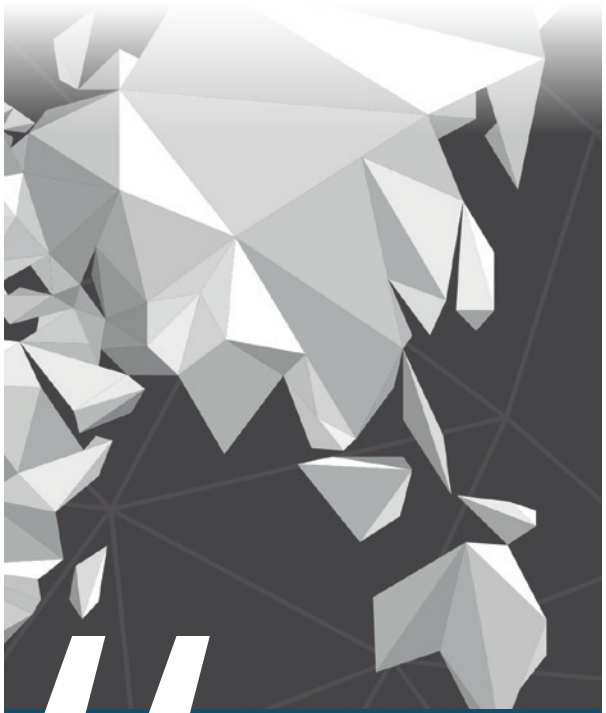
Q. Could you provide an insight into recent trends shaping financial crime in South Africa? How great a risk does financial crime, such as money laundering, now pose to companies?

A: Weakly controlled access to state assets and country resources in the context of significant levels of wealth and income inequality, as well as weak institutions and a financial services and communication services sector with significant infrastructure and geographical reach, provides fertile ground for financial crime in the context of converting property to own use. High levels of criminal intent to strip South Africa of its resources exist in a pliable environment to convert such property to own use. Efforts by financial institutions to resist these efforts also informs this shape. There is a significant risk of licit and illicit business coexisting in the same ecosystems, supported by the impact of wealth and income inequality and abundant criminal intent. This leads to wide ranging organised crime structures operating in a pliant ecosystem.

Q. In your experience, what are the main types of financial crime that organisations are encountering? What are the typical sources of such risks?

A: There seems to be a pattern comprising the extraction of assets or valuable items illegally, followed by money laundering conduct to layer the source of ill-gotten gains. The root causes and behaviours enabling the extraction of assets are often informed by bribery and corruption, hence nullifying the controls and systems normally mitigating theft and fraud. This seems to be the current way of illegally converting property to own use. What makes money laundering such a significant source of financial crime risk are the immaterial concepts of trust and confidence, to which is now attached a value, in the process of value transfer and layering. This is no different to the concepts of trust and confidence persisting in a functioning banking system, the difference being that, in a functioning banking system, regulatory frameworks and rules render events in the formal transactional banking system more visible and transparent. In the digital world, blockchain also gives a value to trust and confidence, but in a different dimension than the formal transactional banking

KPMG



It is extremely important that future technology developments address the behavioural aspects of financial crime, rather than just its root causes.

and hawala dimension. These levels of invisibility invite different uses for these systems of value transfer, some of which are illicit, or simply visited with common law or statutory illegality.

Q. What legal and regulatory initiatives are set to have a significant bearing on this issue in South Africa? How would you describe the nature and extent of the demands being placed on companies to help reduce financial crime?

A: There are many approaches toward mitigating or eliminating financial crime. Regulation and legal reporting obligations are mostly intended to make these crimes more transparent, but do not necessarily eradicate the scourge. Other approaches centre around education, in a belief that awareness speaks to the natural goodness of humans or that wider knowledge of the issues will somehow deter threat actors. A lot of money goes into these initiatives. Yet another approach, driven by the basic concept of financial crime, which is the conversion of an ill-gotten gain to the estate of a threat actor, suggests the best way to eradicate the scourge is by permanently separating the threat actor

KPMG

from the gain and the productive means needed for the gain. This entails legal and law enforcement action, supported by investigation. In this context, companies can support these interventions by virtue of providing evidence, cutting money laundering activities from their ecosystems, being vigilant, and understanding the threats they face and then acting according to that understanding.

Q. In the wake of enforcement action, do companies need to proactively review and revise their practices?

A: Introspection should follow enforcement action, with a review of practices aimed at combatting money laundering. However, I would argue that successful enforcement action against a company suggests the company has either not been proactive in mitigating financial crime, or at least has not acted lawfully by being non-compliant. When migrating to a proactive posture from a purely compliant attitude, informed by the need to mitigate financial crime as a threat to the trust and confidence in the company, and perhaps in the industry it operates in, practical execution requires a deep understanding of how a financial criminal seeks to exploit the organisation and then react accordingly. It is a question of building your corporate culture in this regard.

Q. How important has technology become in the fight against financial crime? How are innovative AML solutions being used to enhance systems and processes?

A: The sheer size of the transactional universe and the prevalence of financial crime risk makes technology essential in mitigating financial crime. Of course, technology needs to be well thought through and properly integrated with existing operating systems. The current challenges comprise simplifying the solutions, having them operate as an indivisible part of the operating system and, perhaps more importantly, being able to responsibly leverage the data organisations collect. It is extremely important that future technology developments address the behavioural aspects of financial crime, rather than just its root causes. Using technology to vertically analyse multiple layers of data is invaluable when investigating financial crime.

KPMG

Q. Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take?

A: There is probably no one size fits all approach but, having a jurisdictionally relevant protocol which is stress tested and regularly exercised, is critical. Because of the significant implications of falling foul of financial crime, the protocol needs to work effectively. Aspects to consider including in such a protocol are, firstly, an effective investigation programme that generates a deep understanding of financial crime events, and the root causes and behaviours that facilitate them, preceded by an effective triage process enabling an organisation to stop the event and prioritise damage control. Secondly, disclosures legally required to be made for the purposes of effectively mitigating financial crime and its impact are critical. Thirdly, substantive cooperation within industries aimed at mitigating financial crime and its impact is critical to address possible systemic impact.

Q. What essential advice would you offer to companies looking to improve the way they manage financial crime risk? How much of a challenge is it to tailor new innovations to a company's operational realities?

A: The definition of financial crime – converting property to one's own use – belies the complexity and dynamics of the real world. Organisations need to develop a deep understanding of this context by asking themselves some key questions. Why is my business attractive to organised financial crime? Is it because it has assets? Is it because it has infrastructure? Is it because it has a good reputation or unchecked levels of public and counterparty trust? Consider knowing your customers versus really understanding your clients and counterparties. Why is a transport business receiving frequent capital contributions from shareholders, operating with low maintenance expenses and making many payments to a funeral services business? Bribery can have a devasting impact on the controls and systems aimed at combatting financial crime.❑

KPMG

www.kpmg.com

KPMG is a global network of professional services firms providing audit, tax and advisory services. It operates in 147 countries and territories and has 219,000 people working in member firms around the world. The independent member firms of the KPMG network are affiliated with KPMG International Cooperative, a Swiss entity. Each KPMG firm is a legally distinct and separate entity and describes itself as such.

DÉAN FRIEDMAN Director

INDEPTHFEATURE

ANTI-MONEY LAUNDERING

2021

FINANCIER WORLDWIDE corporatefinanceintelligence