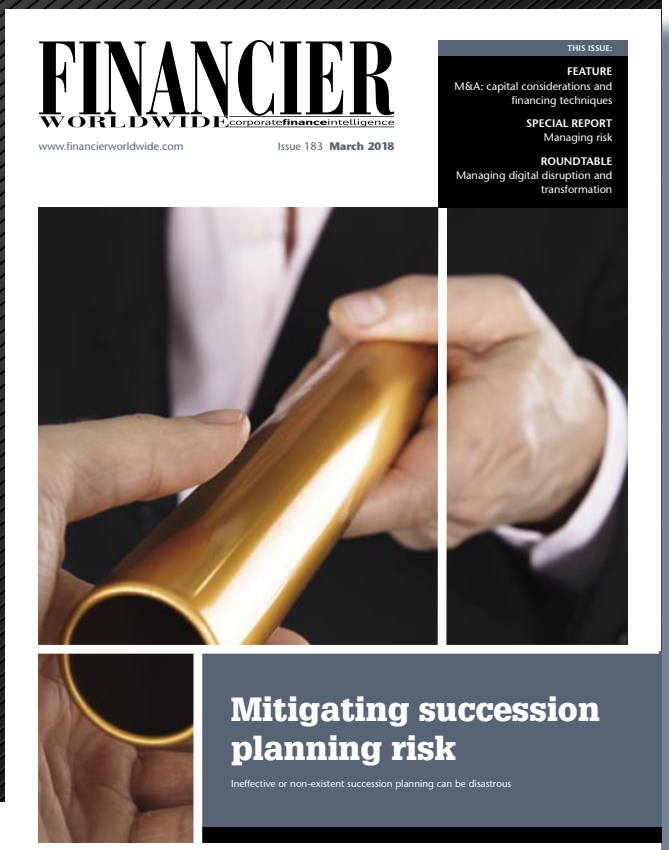
SPECIAL REPORT

FORUM: Managing financial crime risk and AML processes with technology



REPRINTED FROM
MARCH 2018 ISSUE

FINANCIER WORLDWIDE corporatefinanceintelligence

FORUM:

Managing financial crime risk and AML processes with technology

FW moderates a discussion on managing financial crime risk and AML processes with technology between Nick Parfitt at C6 Intelligence, Steven Beattie at EY, Khalil Maalouf at Skadden, Arps, Slate, Meagher & Flom LLP and Kevin Petrasic at White & Case.

THE PANELLISTS

Nick Parfitt
Product Director
C6 Intelligence
T: +44 (0)20 3741 1200
E: info@c6-intelligence.com

Nick Parfitt has 18 years' experience in project and programme management, business process change and implementation of technology and business solutions in leading global financial services, telecommunications and public sector organisations. He also has seven years' experience in financial crime compliance consulting and industry experience supporting Tier 1 financial institutions in assessing their anti-money laundering (AML) and know your customer (KYC) sanctions operations.

Steven Beattie
Principal
EY
T: +1 (212) 773 6378
E: steven.beattie@ey.com

Steven Beattie is a leader of EY's anti-money laundering and sanctions advisory services, and is also EY's global financial crime operations leader, where he leads a global solution focused on delivering innovative, technology enabled teams and services across the full domain of financial crimes operational needs. He stays at the forefront of advising and supporting the industry on the unique and pervasive issues and challenges to build a fully compliant and sustainable financial crime programme.

Khalil Maalouf
Counsel
Skadden, Arps, Slate, Meagher & Flom LLP
T: +1 (202) 371 7711
E: khalil.maalouf@skadden.com

Khalil Maalouf is active in the areas of banking regulation, supervision and enforcement and has represented clients on complex cross-border compliance and enforcement matters, including the resolution of administrative and enforcement proceedings involving federal and state regulatory agencies and prosecutors.

Kevin Petrasic
Partner
White & Case
T: +1 (202) 626 3671
E: kevin.petrasic@whitecase.com

Kevin Petrasic is a banking partner and head of White & Case's global financial institutions advisory practice. He has extensive experience with bank regulatory, transactional, bank insolvency, compliance, supervisory, enforcement, legislative, and policy issues and matters. He advises domestic and international financial services firms, including commercial banks, investment banks, private equity and hedge funds, investment managers and advisers, retail securities firms, insurance companies and payment services firms on a wide array of issues.

FW: Could you provide an insight into recent trends shaping the financial crime landscape? How great a risk does financial crime, such as money laundering, now pose to companies?

Parfitt: It is hard to generalise, because the financial crime landscape varies according to the industry that companies operate in, their jurisdictional risk, the products and services they offer and how mature their compliance operation is. In some cases, it is basic anti-money laundering (AML) failings rather than the crimes themselves that are creating the risks. You would have expected Deutsche Bank, for example, to pick up on the 'mirror trades' that result in it being fined by the Financial Conduct Authority (FCA) and New York Department of Financial Services last year. Recently, the UK Gambling Commission had to warn all 195 UK operators to raise their AML game to protect customers and prevent money laundering. They even identified money laundering reporting officers at some gambling firms with no formal qualifications and an inability to explain what money laundering is. So the risk of financial crime is often being magnified by problems with companies' own controls and procedures. In other cases, new technology is a conduit. In Australia, we have seen intelligent deposit machines, which allow anonymous cash deposits and transfers even when the bank is closed, linked to alleged violations of laws relating to terrorism and crime funding. It will also be interesting to see how cryptocurrencies and regulation shake out in 2018, and what the impact will be of the revised Directive on Payment Services' (PSD2) opening up of financial transaction information with FinTech firms.

Maalouf: We can discern some relevant trends from recent enforcement actions issued by regulators on both sides of the Atlantic. Many of these actions address the common AML and combating the financing of terrorism (CFT) compliance issues that companies face, such as inadequate compliance training and insufficient transaction-monitoring systems.

At a minimum, these actions suggest that regulators will continue to play an active role in addressing the risks that financial crime poses to the industry. Compounding the challenge is the increasing complexity of fraud-related criminal activity and money laundering schemes, particularly with the proliferation of cyber-enabled crimes. While fraud departments have generally focused on minimising financial losses on a linear basis, and AML departments on the provenance of funds, recent cyber events have given rise to a renewed focus on the convergence of fraud and money laundering risks and the tackling of such risks in a coordinated and cross-functional fashion.

Petrasic: Money laundering and related financial crimes pose an ever increasing risk to companies in all industries, but particularly for banks and non-bank firms operating in the financial services space. These risks are increasing both in terms of magnitude and frequency, and most significantly with respect to the sophistication and complexity of the means and methodology employed to carry out the various types of financial crimes we hear about on a daily basis. With numerous and sophisticated bad actors – including nation-states and organised crime networks – actively pursuing financial crime activities, companies require increasingly more sophisticated prevention and detection methods, as well as other tools and means to tackle financial crime. Certainly, one important trend is the rise of technology solutions – FinTech, RegTech and the application of artificial intelligence (AI) tools – specifically designed to combat financial crime, particularly money laundering, terrorist financing and similar financial crimes. While technology is playing a key and effective role in the fight against financial crimes, it is important to bear in mind that robust, comprehensive and periodically reviewed and updated policies, procedures and systems are also critically important measures for financial services firms.

Beattie: Money laundering and financial crime remain critical issues and board-level concerns across the financial services industry. Furthermore, intervention is increasingly becoming a responsibility for non-bank financial services entrants, including alternative payment providers

and innovators in the cryptocurrency space. As long as there is crime, and criminals need to hide their ill-gotten gains, the financial services industry will maintain a front line responsibility to identify and report these activities. In addition to the risk of being implicated in a money laundering scheme, financial services firms face even greater responsibilities and penalties from globally dispersed regulatory authorities. Regulation and compliance continue to evolve, and we have seen a greater focus on financial penalties across the globe for firms that have insufficient programmes or control breakdowns.

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

Maalouf: In addition to 'traditional' financial crimes like fraud and money laundering, recent cyber attacks have highlighted another category of potential crime – cyber crime – against which companies must be vigilant. Notably, the North Korea-linked attack against a major motion picture company destroyed much of the firm's IT infrastructure, and the 'WannaCry' ransomware attack rendered critical data inaccessible at financial institutions (FIs) and government agencies worldwide. More recently, the data breach at one of the three major US credit bureaus was a significant wake-up call for financial services firms and consumers alike. These attacks illustrate a serious systemic risk, and while these examples show risk from external sources, such as third-party bad actors engaging in criminal conduct, it is important to recognise that insider threats or complacency can be just as costly and damaging for firms.

Petrasic: The main types of financial crimes that most organisations encounter involve both sophisticated cyber attacks, as well as less sophisticated cyber intrusions, including phishing scams and similar types of less obvious but still effective intrusions. Often, these attacks are targeted at exploiting weak systems and controls, including outdated and known vulnerabilities that have not been patched, software that has not been implemented properly or effectively, a lack of employee training to understand and use systems effectively, or simply a lack of employee training to understand and avoid situations imposing increased risks of financial crime. In addition, organisations continue to confront more traditional types of financial crime that rely less on technology-based activities. These involve violations of economic sanctions, anti-bribery and corruption and anti-money laundering laws, among others. The typical sources of risks for technology-based crimes include internet hackers, nation states and organised crime groups infiltrating these spaces. Less technology-based crimes include traditional actors, which often include organisation insiders.

Beattie: The main types of financial crimes have not changed substantially, although the methods of money laundering have become more sophisticated and difficult to identify. We are continuing to see criminals engaged in fraud, sanctions evasion, drug trafficking, human and labour trafficking and terrorist finance activities. As financial services firms become more proficient at identifying patterns of suspicious behaviour, criminals become more creative in their methods. A significant challenge is that the source of risk has become even more embedded in the labyrinth of payments and relationships, and financial services firms have a greater responsibility to find the ultimate bad actor in this maze. Complex corporate and beneficial ownership structures, greater reliance on online-only validation of identity, and escalating global payment structures make it more difficult to manage risk and avoid unnecessary vulnerability to attack. The key message is that today's risks are different to prior risks; organisations must remain vigilant to keep pace and fulfil their compliance responsibilities.

Parfitt: 'Mule' accounts and the use of foreign students to launder money in retail banking are real challenges for UK banks. Cyber crime was big in 2017 and likely to remain so this year. Consumers lost £130bn to cyber criminals last year, and we also saw increasingly sophisticated ransomware attacks such as WannaCry and Petya/NotPetya and major data breaches including the high-profile attack on Equifax. Potentially even more worrying is the trend for 'Crime-as-a-Service'. This is where cyber criminals rent out their tools, increasing the volume of attacks. Criminals are also known to be exploring how to use AI and machine learning (ML) in financial crime.

> "FINTECH AND REGTECH APPLICATIONS AND AI SOLUTIONS BASED ON ML MODELS ARE POISED TO HAVE A SIGNIFICANT IMPACT ON FINANCIAL CRIME AND, IN MANY RESPECTS, HAVE ALREADY DONE SO."
>
> KEVIN PETRASIC
> White & Case

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

Petrasic: FinTech and RegTech applications and AI solutions based on ML models are poised to have a significant impact on financial crime and, in many respects, have already done so. For instance, the development of AI applications that can cut through voluminous amounts of data and decipher, from an algorithmic perspective, the risks posed to an organisation and ways to adapt systems to address those risks are providing new insights and augmenting current methods of identifying and managing financial crime risks. These insights can help calibrate an organisation's existing compliance mechanisms and monitoring activities, identify vulnerabilities, assist in improving existing policies and procedures, and help to develop and implement preventative measures to guard against and reduce financial crime risks.

Beattie: The regulatory focus is not stagnant, and we foresee expectation and risk management responsibilities continuing to evolve within the industry. Most recently, in the US, there has been a change in the customer due diligence rule that requires institutions to re-evaluate how they collect and maintain know your customer (KYC) information on their customers. There are also increased identification and reporting requirements related to fraud, with the majority of this responsibility falling to FIs. Interestingly, many of these increased expectations are driven by industry events. For instance, the Panama and Paradise Papers sent a strong message across the industry that ultimately increased the focus on offshore financial dealings and tax evasion. The increased prevalence of virtual currencies and the use of Bitcoins to satisfy ransom demands or fund terrorists are just two recent examples of events that will continue to drive change.

Parfitt: The UK's corporate criminal offence of the failure to prevent the facilitation of tax evasion, which came into law as of September 2017, has potentially far-reaching implications and extraterritorial reach. It is similar to the UK Bribery Act (2010) but requires significant organisational assessment, evaluation and process implementation in order for companies to be compliant. Infringements have a material impact on both the organisation and individuals. If Tier 1 banks are still being fined over basic AML and CTF breaches, then they are clearly struggling to achieve compliance with current regulations, let alone the slew of additional regulations. For smaller firms, this can be even more challenging both from a cost and revenue point of view, as new headcount is needed to satisfy the organisational control requirements – even before the necessary changes to processes, technology and governance are put in place. I also expect anti-bribery and corruption to be high on the agenda of compliance practitioners given the reputation of Charles Cain, the new head of the Foreign Corrupt Practices Act (FCPA) at the Securities and Exchange Commission (SEC). He is well known for pursuing non-US companies in a bid to 'level the playing field'. A 2017 EY survey showed that 5 percent of respondents to its biennial study of bribery and corruption across Europe, the Middle East, India and Africa still perceive that the problem is widespread in their country.

> "AS GATEWAYS TO NATIONAL AND INTERNATIONAL FINANCIAL MARKETS, FIS ARE UNDER TREMENDOUS PRESSURE TO HELP COMBAT FINANCIAL CRIME."
>
> KHALIL MAALOUF
> Skadden, Arps, Slate, Meagher & Flom LLP

Maalouf: Lawmakers have taken steps to modernise their respective AML and CTF frameworks, in both the US and Europe, through new or amended legislation and regulations. Examples include the EU's fourth AML Directive, FinCEN's new CDD requirement, and the New York State Department of Financial Services' Part 500 and Part 504 certification requirements. These steps reflect the growing focus on cyber security and risk-based approaches to compliance processes like customer due diligence and transaction monitoring and filtering. As gateways to national and international financial markets, FIs are under tremendous pressure to help combat financial crime. Firms have dramatically increased compliance staffing to reduce the likelihood of running afoul of the law. Effective compliance, however, requires more than increasing staffing levels on an absolute basis. FIs must address vulnerabilities thoughtfully, on a risk basis, in order to minimise compliance risks in practice. FIs should also adopt a holistic view in managing risks across their businesses and consider ways to take advantage of synergies between their compliance and risk management operations.

FW: In your opinion, to what extent are the anti-money laundering (AML) and financial crime controls typically deployed by organisations simply inadequate to the

task? Can new technology help to address such shortcomings?

Beattie: We do not believe, generally speaking, that controls within financial services are inadequate to the task, although they must constantly be evaluated and evolved. A number of firms have made massive investments in improving 'the basics' – knowing their customers, monitoring their activity and increasing quality of reporting, for instance. That being said, many firms have underinvested, or not made their AML programmes a firm priority. Thus, we still see bad actors thriving with the laundering of their ill-gotten gains throughout the industry. The use of emerging and innovative technology, increasing the quality of data and leveraging public sources of data for validation, are all critical strategies for success. A word of caution, however: buying technology does not solve the issue. We have seen numerous cases of firms running technology 'out of the box' and not customising it to their unique products, clients and delivery channels. These turnkey strategies, generally, are not successful in satisfying the control objectives of these firms.

Maalouf: US and EU regulators have recently cited organisations for inadequate AML systems and controls, which further underscores the need for compliance professionals to ensure the right combination of IT solutions and analytical tools to stay ahead of an evolving threat environment. While there has been an evolution of these systems to combat financial crime, including the use of behaviour-detection logic, the integration of correlated data sources, pattern-recognition algorithms and the centralisation of case management systems, organisations need to know how to employ the technology effectively and holistically. In addition, in an era of Big Data, companies face greater expectations regarding their ability to consolidate and capitalise on the information available to them in order to minimise fraud and AML risks.

Parfitt: The challenge with AML compliance is that end-to-end process is highly nuanced, resource-intensive, porous and organisationally far-reaching. Plus, there are high expectations that technology can automate a lot of the necessary controls and reduce operational costs. To date, technology has provided benefits in certain areas but has fallen short of achieving true transformation. However, there is no shortage of new technological approaches that could achieve this: AI, ML and digital IDs using blockchain technology have the potential to revolutionise the industry, but are still a way off being business as usual (BAU) processes. Better adoption of biometric technology could provide material improvements in onboarding, screening and business relationship monitoring. It has a much lower barrier to entry than implementing AI and ML into the due diligence process.

Petrasic: Most regulated organisations, such as FIs, have in place robust AML, Bank Secrecy Act (BSA), and sanctions detection systems. Electronic commerce, however, remains susceptible to financial crime. Even when systems comply with applicable laws and regulations, they may not be up to new challenges not contemplated by an outdated legal or regulatory framework. Consequently, compliance with legal requirements may not always equate to having systems in place that work in practice. For instance, KYC requirements and rapidly emerging know your customer's customers (KYCC) standards are becoming increasingly more challenging for companies. In addition, it is becoming more costly for some institutions, including money service businesses and vendors, to monitor cyber crime and other activities, which, of course, can have significant implications for financial services firms in managing financial crime risks on both the customer side and vendor side of their operations.

FW: How important has technology become in the fight against financial crime? What, in your opinion, have been the most innovative AML solutions seen in recent times?

Maalouf: With bad actors constantly innovating and seeking out new methods to carry out their crimes, organisations must strive to stay one step ahead. Technology is playing an integral role in this fight. For example, many companies are considering AI and ML to enhance their various AML compliance processes. AI and ML can connect business lines, identify nonlinear relationships and compress the compliance decision tree, allowing for effective staffing, predictive analyses, reduction in false positives and, ultimately, quicker resolution of alerts. As another example, blockchain

> "WITHOUT SOPHISTICATED TECHNOLOGY, MANY FIRMS ARE BURDENED WITH EVER-INCREASING PEOPLE COSTS THAT ARE NOT OFFSETTING THE RISKS."
>
> STEVEN BEATTIE
> EY

technology offers a means of creating an encrypted KYC registry that firms can continually update and access. The distributed nature of the database would improve data availability, as information is moved out of silos and onto a shared platform. These tools provide for a smarter, safer system and reduce an institution's compliance and opportunity costs.

Parfitt: Technology is a key enabler. But unless the business problem is clearly articulated and addressed, adoption and results can be poor. We have seen some innovative approaches from RegTechs, mostly in the customer onboarding space, where they are providing a more seamless ability to bring multiple risk databases together with corporate registrars. Where we still see a lack of disruption is in the high volume batch monitoring and payment filtering spaces, where legacy systems remain very difficult to displace. In these areas, RegTechs have been able to create tools that sit on top of legacy software providers to bring value.

Petrasic: Technology plays a critical but not exclusive role in the fight against financial crime. As financial crime actors use increasingly complex tools, technology can help and must be deployed effectively to control for such threats. Organisations must nevertheless have systems to fill in gaps as well as understand that there are less technological ways to exploit vulnerabilities – including unsophisticated controls – that are not always understood when systems are being designed and may be manipulated to hide criminal activity. One notable example includes the Bangladesh Bank heist, whereby the central bank's credentials for payment transfers were compromised and illegal transfers were made. Part of the criminal activity involved shutting down a printer control that would have otherwise tipped off the central bank if it was operational. As a result, it took longer than normal to detect the intrusion and cancel all of the transfer activity, contributing to the loss of millions of dollars.

> TO DATE, TECHNOLOGY HAS PROVIDED BENEFITS IN CERTAIN AREAS BUT HAS FALLEN SHORT OF ACHIEVING TRUE TRANSFORMATION. HOWEVER, THERE IS NO SHORTAGE OF NEW TECHNOLOGICAL APPROACHES THAT COULD ACHIEVE THIS.
>
> NICK PARFITT
> C6 Intelligence

Beattie: Technology has become critically important as a tool for financial services firms as payment methods and client onboarding strategies have become more technology-enabled. In addition, technology is crucial for dealing with the massive volume of activity channelling through the industry. Without sophisticated technology, many firms are burdened with ever-increasing people costs that are not offsetting the risks. FIs are increasingly employing RPA solutions to improve quality and workflow, integrated automation, analytics and ML to enhance investigations, as well as successful strategies using advanced analytics and Big Data solutions to monitor client activity. Companies that are able to implement innovative technologies with alternative people models allow lower cost, as well as higher quality onshore and offshore managed services solutions. This is a rising trend in the industry to offset unsustainable spend and increase overall quality. Companies must exercise caution around technology, however. They should be careful to avoid the hype of unproven solutions. This is an area where measured approaches to innovation can increase quality while not introducing unnecessary regulatory or risk issues.

FW: Once a company suspects or confirms it has fallen victim to financial crime, what initial action should it take? At this stage, can technology be utilised to mitigate extensive financial and reputational damage, for example?

Beattie: This issue is more common than one may think, as the industry has a track record of both successful and unsuccessful action steps. The first step companies should take is to determine the extent of the issue. Was it a one-time event? Does it represent a systemic issue across the organisation? Is the financial crime still ongoing as you undertake your investigation? Organisations then need to understand the root cause. Was this a new method of laundering requiring changes to monitoring strategies or a breakdown of well-documented controls? In all of these cases, technology, in particular visual analytic and data manipulation tools, can be used to accelerate forensic analysis and to help guide companies toward strategies for future risk avoidance. Of course, organisations must also consider their need for outside assistance for significant events, sources for industry common and best practices and whether they should engage with legal counsel or discuss the issues with their regulatory authorities. These decisions are made based upon the severity and extent of the financial crime issue.

Petrasic: There is an array of important considerations in connection with responding to a financial crime, including

the type of crime involved. A company should consult professionals, and consider having a team on retainer, including legal, accounting and forensics experts, to assist in investigating an incident to understand its scope and the organisation's vulnerability and potential liability. Companies should also engage law enforcement with the assistance of counsel to report the crime and get help in trying to identify and pursue the criminal actors. An important consideration in this regard is to avoid tipping off money launderers, cyber thieves and other financial crime actors, as well as taking appropriate steps to preserve any trail that may lead back to the criminal actors. If the financial crime involves a cyber security attack, the company should also immediately reach out to its insurance or cyber insurance carrier. Depending on how effectively an organisation deploys technology, it may mitigate financial or reputational damage caused by financial crime incidents.

Parfitt: If it falls victim to a financial crime, an organisation should self-report to its regulator and ensure that this becomes a board-level agenda point. Depending on the nature and scope of the incident, external counsel and expertise may need to be sought. It will also be necessary to ensure internally clear governance and ownership for resolution.

Maalouf: When faced with a cyber event, an organisation's first steps should be to secure IT systems and isolate compromised network segments to prevent further damage to the company's IT and digital assets. Incident response teams should not be limited to IT and data experts, but should also include communications and legal team members to proactively manage the reputational, notification and legal considerations that arise. Efficient data management is integral to any response, both in terms of speed and cost.

FW: What final advice would you give to companies on selecting and deploying technologies to help manage the risk of financial crime? How much of a challenge is it to tailor such systems and programmes to a company's operational realities?

Petrasic: In order to effectively select and deploy technologies to help manage financial crime risk, companies should consider the following. First, understand what the technology can and cannot do. Second, use more than one solution, both technology-based and traditional solutions. Systems should be layered, and to some extent, redundant, allowing for a risk-based approach and business continuity following a major incident. Third, ensure that technology is fully implemented and maintained – employees should be well trained and well informed on what information the system needs to operate effectively, and the board of directors, or a committee, should be accountable for and engaged on these issues and responsible for taking appropriate action. Fourth, keep technology up-to-date, including by checking vulnerability reports. Fifth, understand best practices and discuss such practices with peer organisations. Finally, share information regarding financial crime efforts and initiatives with peer organisations. Hiring and retaining the right personnel is also a key issue. It can be a significant challenge for an organisation's chief technology officers to collaborate effectively, understand specific system requirements and analyse whether such systems are functioning properly, including by monitoring them on a real-time basis.

Parfitt: Do not try and boil the ocean. Assess the highest risk areas to which technology can add value or identify lower risk processes where automation will not result in material breaches. Have a plan and a roadmap, assign ownership and ensure there is appropriate organisational focus and commitment. Every organisation is different and no one size fits all. Operational constraints need to be clearly factored into the realities of implementing change and should be aligned with businesses strategy and priorities.

Maalouf: Technology should be deployed strategically, and in a manner consistent with a company's comprehensive assessment of its specific financial crimes risk. Tailoring systems and controls to effectively address the threat of financial crime is a challenge, and there are a variety of approaches that organisations can take. Ultimately, the optimal structure depends on the specific risks the organisation faces and is related to the broader discussion on the placement of compliance within the corporate structure. The approach may be to centralise the relevant compliance staff into a financial crimes unit, or to maintain specialised fraud and AML units, but provide for cross-training and information sharing to prevent them becoming siloed and less effective. Overall, the central component is to ensure both vertical and horizontal coverage of fraud, cyber and AML issues at the company.

Beattie: Financial services firms need to remain aware of their unique responsibilities in the war on financial crime. That being said, in selecting technologies, there needs to be an understanding that no one technology is a best fit across all businesses, products and client types. One should first weigh any technology against its compatibility and track record with your business. It is also essential to customise technologies to best meet your organisation's needs. This is a significant challenge, given that most firms have pervasive data quality issues, lack of integration of their existing operational systems and tight budgets in a competitive landscape. Drawing upon the experience of your peers or outside firms who have experience with these topics is the fastest accelerant to separating the 'hype' of the next new technology from the reality of the obligation to continue as the front line of defence. Smart spending, focused on key risks and relying on proven innovation, is just one way to stay one step ahead of money launderers while still satisfying the key objective of better serving your underlying clients. ■