ROUNDTABLE November 2021

CORPORATE FRAUD

Corporate fraud is a significant ongoing challenge for many companies, with instances of bribery, corruption and money laundering rising exponentially. Moreover, the rapid development of technology has caused cyber-related corporate fraud to evolve, allowing malicious actors to successfully penetrate many companies' control frameworks or security infrastructures. A further threat to business resilience is the new landscape formed by COVID-19 – a time of crisis and change and a perfect storm for corporate fraud. ■

THE PANELLISTS

Tapan Debnath
Head of Integrity, Regulatory Affairs & Data Privacy – Process Automation, ABB
T: +44 (0)7342 089 528
E: tapan.debnath@gb.abb.com
www.abb.com

Tapan Debnath is a UK qualified lawyer with 18 years' post qualification experience. He specialises in corporate compliance and internal investigations. He is Head of Integrity, Regulatory Affairs and Data Privacy for the Process Automation Business area of ABB Ltd. He previously worked at Nokia Corporation in various senior compliance and investigation roles, prior to which he was an investigator and prosecutor at the Serious Fraud Office.

Nick Robinson
Senior Managing Director, Ankura
T: +852 2233 2500
E: nick.robinson@ankura.com
www.ankura.com

Nick Robinson has over 30 years' experience, including 15 years at the partnership level with Big Four forensic teams, dealing with client matters across the integrity spectrum in both Asia Pacific and the Middle East. He also has in-house experience with a US multinational retail corporation where he ran its global procurement investigation team. He began his career with the Royal Hong Kong Police, attaining the rank of detective senior inspector with the Commercial Crime Bureau.

Robert Sikellis
Vice President & US Head of Litigation, Novartis
T: +1 (862) 223 0780
E: robert.sikellis@novartis.com
www.novartis.com

Robert Sikellis is head of US litigation for Novartis where his responsibilities include overseeing internal investigations. Prior to joining Novartis, he was chief counsel for compliance at Siemens, where he oversaw all internal investigations. He started his career as a prosecutor in Massachusetts.

Sarah Foley
Deputy Compliance Officer and Director of Compliance, Patterson Companies, Inc.
T: +1 (651) 405 5116
E: sarah.foley@pattersoncompanies.com
www.pattersoncompanies.com

Sarah Foley is deputy compliance officer and director of compliance for Patterson Companies, Inc. In this role, Ms Foley has responsibility for the company's global ethics and compliance programme, initiatives and strategy.

Fran Marwood
Forensics Partner, PwC UK
T: +44 (0)7841 491 400
E: fran.marwood@pwc.com
www.pwc.com

Fran Marwood leads PwC UK's Digital and Forensic Investigations practice. He has given support to companies, and their stakeholders, to investigate and navigate crisis events, for 25 years. Typically, these need an expert independent review to establish the facts. Mr Marwood's personal areas of experience are as a forensic accountant and fraud expert, leading complex investigations across both the UK and numerous emerging markets.

John Hartley
Partner, Shoosmiths
T: +44 (0)20 7282 4068
E: john.hartley@shoosmiths.co.uk
www.shoosmiths.co.uk

John Hartley specialises in advising individuals and corporates through the challenges of criminal and regulatory investigations from beginning to end. He joined Shoosmiths in 2019 from Hodge Jones and Allen where he was head of financial crime and regulatory investigations. He has extensive experience advising on complex cases brought or contemplated by agencies such as the Serious Fraud Office (SFO), National Crime Agency (NCA), Financial Conduct Authority (FCA), Crown Prosecution Service and HMRC.

FW: Could you describe the main types of corporate fraud that you are typically seeing across the current financial and economic landscape?

Debnath: Corporate fraud is a cross-sectoral, cross-industry crime which is high on the list of risks to combat for most companies and financial institutions. Identifying, investigating and prosecuting corporate fraud is also high on the enforcement agenda of regulators and law enforcement around the globe. There has, however, in recent years been a decline in bribery and corruption enforcement by the US Department of Justice (DOJ) and the UK Serious Fraud Office (SFO). In 2020, the DOJ fraud section charged 32 percent fewer individuals than in the preceding year. Tax enforcement actions in the US and Europe are, however, on the increase. For example, divided stripping, or 'cum-ex' trading, in which multiple parties exploit a tax loophole which allows both seller and buyer to claim the same tax refund, is gaining enforcement traction. The UK's Financial Conduct Authority (FCA) is investigating approximately 14 financial institutions and six individuals, and authorities in Germany, the Netherlands and Denmark, for example, are also taking enforcement action in this space.

Foley: Although there has not been much divergence from the general corporate fraud concerns seen in recent years, such as bribery, corruption and money laundering, the rapid development of technology has caused cyber-related fraud to evolve, allowing malicious actors to successfully penetrate many companies' control frameworks or security infrastructures. Fraud is also emerging through the misuse of data and many companies' inability to effectively protect sensitive data and information. Data protection should be a particular priority for companies that operate in industries where the collection, processing and transfer of highly sensitive personal, health and consumer information occurs. It is critical for these companies to ensure systems and procedures are implemented in a manner that is robust enough to counter these risks and proactively protect against fraud.

Marwood: Our biennial 'Global Economic Crime Survey', which has been running since the early 2000s, gives us some really valuable insights into fraud trends. The top five fraud types reported in the latest issue were asset theft, bribery, accounting misstatement, customer fraud – where fraudsters use the customer channel to defraud a business, such as a mortgage fraud – and cyber crime. Looking through the lens of the 'fraud triangle', the COVID-19 pandemic has created a very favourable environment for the fraudster. New opportunities opened up to commit fraud as organisations moved to work in a remote environment and existing internal controls, such as approval processes, were stretched. Significant incentives to commit fraud arose out of concerns for business survival, as well as from the very large sums of government support being made available. Moreover, fraudsters have been able to more easily rationalise their actions due to 'exceptional' circumstances.

Sikellis: In the pharmaceuticals industry, the focus on potential fraud remains constant, including interactions with healthcare professionals, government health authorities and providers from clinical development through initiation of therapy by patients. We expect regulators to continue to examine these issues from a local, regional and global level. To be sure, as we emerge into a post-pandemic world, the disparities in healthcare will continue to result in broad areas of enforcement. Pressure on drug pricing and access to medicines will likely increase. This, in turn, will result in corporate challenges to bring new medicines to patients in a more efficient, cost-effective, and expeditious manner and could result in individual misconduct if shortcuts are inappropriately taken. This could impact a range of areas in the industry, including good manufacturing processes, reliability of data before approval agencies and distribution channels. Regulators and enforcers will likely examine potential risk areas that are ripe for conflicts of interest, fee-for-service and compensation models throughout the system – from clinical trials to promotional initiatives – and the variety of issues relating to access to medicines.

Hartley: Typically, money laundering is the main type of corporate fraud we see in the financial services sector. Last year the UK's National Crime Agency (NCA) processed over 570,000 suspicious activity reports (SARs), an increase of 20 percent from the previous 12 months. In addition, there was an 80 percent increase in requests for a defence against money laundering (DAML). This is clearly demonstrative of where fraud is on the increase. History has shown us that in times of crisis and change, fraudulent activity will increase with opportunity. And now, with the changing landscape thrust upon us by the COVID-19 pandemic, opportunity has arguably never been greater. We need to be aware that new types of fraudulent activity will emerge. The new and sometimes confusing processes associated with the furlough scheme will no doubt bring rise to some cases of fraud. Although accidental overpayments will be recovered by HMRC as taxable income, there will be cases where fraudulent parties have attempted to take advantage and there will be prosecutions for the most serious offending.

Robinson: With the disruptions brought about by the COVID-19 pandemic, risks have heightened in the following areas. First, impersonation, identity theft and account takeover. Cyber security has not always kept up with rapid digitalisation or the pivot to work from home arrangements. As a result, we have seen an increase in identity theft compromises resulting from sophisticated social engineering tricks that manipulate users into giving away sensitive information. Second, employee fraud. Some employees are taking advantage of the work from home 'new normal' to steal company data or put in fraudulent expense claims. Third, supply chain fraud. The scramble to keep supply chains open has increased workarounds that lead to onboarding new suppliers or third parties that are not fully screened or evaluated. Procurement fraud, with fictitious or duplicate invoices, is also

on the rise. Finally, financial statement fraud. Ongoing pressure to perform despite the disruption is encouraging falsified financial accounts and the manipulation of revenue recognition.

FW: Could you highlight any recent, noteworthy cases of corporate fraud which caught your eye? What would you say are the most important lessons that the corporate world can learn from the outcome of such cases?

Foley: A notable corporate fraud case is 'Operation Car Wash', arguably one of the largest bribery cases in the world. It stands out because of the reach it had beyond Brazil and the complex fraud schemes employed by companies entangled in the matter. This case placed a spotlight on institutionalised corruption across local and multinational organisations. As a result of this case, companies were forced to assess the risk of conducting business in Brazil, which, in some cases, resulted in companies exiting the Brazilian market altogether, or changing their operating model and how it goes to market in the country. This case has served as an important reminder for compliance professionals about the importance of maintaining a robust compliance programme, which meets regulatory expectations and requirements. It is also critical that the expectation of operating with integrity is pushed throughout the organisation from top and middle management. Operating with high ethical values and integrity is not only a competitive differentiator and good for profitability, but also the right thing to do.

Marwood: We see a broad range of corporate fraud cases which are not in the public domain. Themes often repeat and the following publicly-reported cases demonstrate common frauds that we see affecting companies. Three reported cases that illustrate these themes are Hin Leong Trading, where there have been allegations of forgery to secure funding. Airbus, which resulted in $4bn in global penalties to settle allegations of 'pervasive' bribery to secure sales. And Colonial Pipeline, which involved a ransomware cyber attack that shut down a pipeline carrying 45 percent of all fuel consumed on the East Coast of the US. These sorts of issues often stem from problems with related control environments. A key lesson is to make appropriate investment in identifying fraud risks, ensuring appropriate fraud prevention and detection measures are then in place. Counter-fraud technology is playing an increasing role in this area. It is also really important that appropriate diligence and healthy scepticism is applied to key business partners and transactions.

> "REGULAR MONITORING OF FRAUD RISKS, REVIEWING TRANSACTIONS FOR RED FLAGS AND CONDUCTING DUE DILIGENCE ARE VITAL MECHANISMS ALL COMPANIES SHOULD EMPLOY TO COMBAT FRAUD."
>
> JOHN HARTLEY
> Shoosmiths

Sikellis: Amid the devastation of the opioid epidemic, the Purdue Pharma case has been notable both for the troubling underlying facts but also as an example of the dogged pursuit of corporate misconduct by regulators. Late last year, on 24 November 2020, Purdue Pharma LP pled guilty to violating the Food, Drug, and Cosmetic Act, and the Federal Anti-Kickback Statute. As the DOJ noted, "Purdue admitted that it marketed and sold its dangerous opioid products to healthcare providers, even though it had reason to believe those providers were diverting them to abusers". The Purdue case demonstrates a failure of the company to keep patients at the centre of its mission. The case also underscores how a company's reputation can be irreparably harmed, and a company destroyed, when profits are put above the wellbeing of the patients. Purdue is a vivid example of how a company's misconduct can lead to great detriment to society and, ultimately, the downfall of the corporation.

Hartley: The most notable UK case in recent history involves NatWest Bank in relation to offences under the Money Laundering Regulations 2007. The FCA commenced criminal proceeding against NatWest in March 2021 as it believes the bank failed to monitor and properly scrutinise certain suspicious corporate account transactions. We are due to hear soon whether there will be a wider use of the 'failing to prevent' offences that were introduced for corporate bribery and tax evasion. It is important to note that this is the first criminal prosecution against a bank by the FCA under the Money Laundering Regulations 2007. This demonstrates an aggressive shift in the FCA's approach to dealing with companies that fail to prevent fraud. The FCA is showing that it will not allow banks to foster a lax approach when it comes to criminal proceeds. Systems and technology are available to banks to ensure they have tough anti-money laundering defences, and these must be implemented. We have not yet seen any specific prosecutions arising as a result of the COVID-19 pandemic, but it is anticipated that this will change in the coming months.

Robinson: There have been a number of noteworthy fraud cases. Wirecard involved financials manipulation to fabricate revenue and management fraud whereby cash was stolen by the chief executive and other top management. In Kangmei Pharmaceutical, fraudsters used fake bank bills to inflate deposit figures, falsify reported revenue and transfer funds to trade its own stock. Hin Leong Trading involved management fraud, including fraudulent disbursements and forged documents to finance debts. These cases are examples of 'collusive fraud'. This suggests that regular fraud awareness training for all employees – including those onboarding – is vital. The more people are involved in a fraud, the more likely others are to notice. This is where organisations with strong whistleblowing procedures, where code of conduct, conflict of interest and anti-bribery and corruption policies are top of mind, are more likely to uncover fraud attempts before they happen. Leaders should create a positive culture by being open and transparent around potential issues within the company, engaging employees in fraud conversations and sustaining an incentive system that rewards whistleblowers.

Debnath: The extraterritorial reach of the UK Bribery Act 2010 was confirmed in a judgement handed down in the 2020 deferred prosecution agreement (DPA) between the SFO and Airbus SE, which was part of a coordinated settlement with French and US authorities. This was the first UK DPA to apply to a non-UK company where there had been no conduct that could have consisted of the 'actus reus' of the underlying offence taking place in the UK. The test applied was 'carrying on a business' in the UK, which the parties agreed as part of the DPA was the UK nexus. The court did not examine the test in any detail but found that the parent company's "strategic and operational management" of UK subsidiaries was the UK nexus. The takeaway is the confirmation of the Bribery Act's extraterritorial reach – the non-UK parent company management of a UK subsidiary may bring the parent within the ambit of the Act, even where the relevant conduct takes place outside the UK.

> "CULTURES WHICH ARE CLOSED, SECRETIVE OR BLAME-BASED – WHERE MISTAKES ARE PUNISHED – ARE OFTEN ONES WHERE FRAUD THRIVES."
>
> FRAN MARWOOD
> PwC UK

FW: What advice can you offer to companies in terms of implementing and maintaining a robust fraud risk assessment process, with appropriate controls to detect potential misconduct? For example, what measures should they take to strengthen processes around third-party relationships?

Marwood: An organisation's fraud risk assessment is its most important tool for effective and efficient fraud risk management. All counter-fraud activities, such as preventative controls, training, detection and investigation, among others, should be driven by the assessment so they are proportionate, prioritised and tailored to specific fraud risks. While generic counter-fraud activities do provide some baseline benefits, it is often hard to demonstrate to stakeholders how these address the most concerning fraud risks faced by an organisation. From our experience, we see that organisations are not undertaking fraud risk assessments regularly enough or in sufficient depth. These should be reviewed both on a periodic basis – at least annually – and at trigger events, such as an acquisition or new product launch, bringing together perspectives from key operational staff as well as individuals experienced in fraud matters, so that suitable scepticism is brought to bear.

Sikellis: Having a clear and solid ethics, risk and compliance framework is non-negotiable in our view. While policies, guidelines, controls and incentives have an important place in an organisation, we recognise that they will be most effective if they are supported by a cultural environment, leader and manager behaviours, and the implicit and explicit goals that are set. Ethics, risk and compliance should partner with other corporate functions to enable associates to do what is right as integrity and compliance are owned by each of us, regardless of role. As a global company, our resilience in challenging times is directly related to our ability to detect risks early and to mitigate, monitor and remediate them. We will only be able to successfully implement an effective and efficient compliance system if our associates are aware of the company's risk exposure and personally own responsibility for managing risks. In our interconnected world, third-party compliance has an increasing impact on our reputation. Society expects us to be ethical not only through the actions of our own associates, but also through how we select and engage with suppliers and other third parties that work with us. This requires a

strong and agile risk assessment process to identify emerging as well as continued industry risks.

Hartley: Fraud risk is always present, externally and internally. Companies are expected to have practices in place to measure and deal with the risk of fraud. Communication is key. Training and regular updates on all types of potential fraud are essential. Regular monitoring of fraud risks, reviewing transactions for red flags and conducting due diligence are vital mechanisms all companies should employ to combat fraud. At the moment, corporates are criminally liable for failing to prevent bribery and tax evasion, and the only defence available to companies when such fraud has occurred is to demonstrate they have adequate procedures in place and these procedures have been followed and monitored. It is possible that corporates may, over time, become liable for wider economic crimes. When dealing with third parties, companies should ensure their contracts with third-party suppliers include clauses which place an onus on these third parties to comply with legislation to the same standard to also detect potential misconduct. Clauses covering fraud prevention, the anti-facilitation of tax evasion, bribery and corruption and modern slavery should be standard in all third-party contracts.

Debnath: Third parties pose one of the biggest fraud and corruption risks that a company is ever likely to face. Research shows that around 90 percent of Foreign Corrupt Practices Act (FCPA) enforcement outcomes involve third parties in some shape. Depending on the go-to-market model, a company's distributors and resellers are often at the customer-facing end of multi-million-dollar projects. Those third parties may not necessarily hold protection of the company's brand and reputation as sacrosanct as the company itself, instead seeking to win the deal at any cost. That is why it is imperative to have a risk-based third-party screening and monitoring programme. Doing so will allow enhanced due diligence to be performed on higher risk third parties and transactions, with ongoing monitoring as appropriate. Of course, it is necessary to be balanced in such matters and always keep in mind that the company needs to win deals to be successful, and that the compliance function must be seen to be and act as a trusted partner to the business, rather than the proverbial 'office of no'.

Robinson: When implementing a robust fraud risk assessment process, companies should start by taking a fraud health check to identify the organisation's vulnerability to fraud and corruption. Second, assess your whistleblower programme to see whether it supports a 'speak up' culture. Third, use an internal audit to assess the effectiveness of your fraud risk management framework. Finally, use a third-party compliance assessment to identify and mitigate third party non-compliance risks. To this final point, be aware that the main fraud and corruption risks that can emerge from third-party relationships would include potential conflicts of interest with employees, cross-ownership between third parties, history of regulatory violations, litigation records – civil and criminal – and suspicious business scope and scale. We recommend making use of data-driven tools to identify possible third-party fraud, which for instance combines portfolio-level risk screening of suppliers with spend analytics to identify possible cash leakage or cost savings.

Foley: There is no 'one size fits all' approach to a fraud risk assessment frameworks and processes. An effective risk assessment framework keeps tabs on emerging risks – and how those risks are relevant to a company's operations – and maintains a flexible roadmap for mitigation, monitoring, reporting and remediation. It is also important to consider expanding fraud risk assessment teams, as many companies keep the risk assessment team roster limited to management. By incorporating individuals who may not be in a senior role, companies can obtain broader perspectives on how controls are implemented and performing. It also provides an opportunity to train these individuals – who are often seen as 'gatekeepers' – on how to identify, mitigate and report 'red flags'. With respect to third parties specifically, they can pose exceptional risks to an organisation, demonstrated through bribery, asset misappropriation, tax evasion, money laundering and cyber breaches, among others. Therefore, it is critical for companies to establish and maintain effective risk identification and management processes specific to the engagement of third parties. This can

> "THE RAPID DEVELOPMENT OF TECHNOLOGY HAS CAUSED CYBER-RELATED FRAUD TO EVOLVE, ALLOWING MALICIOUS ACTORS TO SUCCESSFULLY PENETRATE MANY COMPANIES' CONTROL FRAMEWORKS OR SECURITY INFRASTRUCTURES."
>
> SARAH FOLEY
> Patterson Companies, Inc.

be accomplished through procurement procedures that outline and implement effective control measures that address cost and understand with whom the company is ultimately conducting business, and strong contracting that permits compliance training, auditing and acknowledgements. Furthermore, an effective, risk-based due diligence programme can also successfully identify third-party risks to an organisation at the outset of and throughout the engagement, through ongoing monitoring activities.

> BEHAVIOURAL SCIENCE, DATA SCIENCE AND DECISION SCIENCE GIVE US A UNIQUE OPPORTUNITY TO ANTICIPATE AND ADDRESS THE TRUE DRIVERS OF ETHICAL AND UNETHICAL BEHAVIOURS.
>
> ROBERT SIKELLIS
> Novartis

FW: In what ways is technology, such as data analytics, helping companies manage the risk of fraud? Are you seeing a rising appetite among companies to explore these solutions?

Sikellis: Behavioural science, data science and decision science give us a unique opportunity to anticipate and address the true drivers of ethical and unethical behaviours. More specifically, behavioural science helps us understand the true drivers of ethical and unethical behaviours and helps us remove the blockers. Similarly, data science helps to draw conclusions and make inferences and predictions across large, disparate and uneven organisational data sets. Lastly, decision science helps transform our insights and evidence into business outcomes by understanding the decision-making process. We use these tools to provide a solid diagnostic of the real situation, in practice, of whether our associates are enabled to do what is right. And, over time, to provide practical, tailored and science-based solutions to an environment that supports our people to do so. While not a 'silver bullet', in a digital era where technology advancements occur at a rapid pace, a company's sustainability will greatly relate to its ability to effectively use technology, such as data analytics, to assist with prompt detection of fraud.

Hartley: We are seeing a rising appetite among companies to explore and implement technological solutions. A quick google search will reveal the large amount of artificial intelligence (AI) and software-based solutions now on offer. It will not be long before AI becomes a staple of the due diligence landscape. The drive for operational resilience in regulated businesses is an issue though, and firms are conscious that there is a significant responsibility in ensuring their AI capabilities can still operate effectively in difficult times. The market is responding to the increased demand for them. Such technological tools can provide myriad functions, including analysing daily transactions and identifying anomalies in data. These automated functions alleviate these onerous burdens from staff. They can be expensive but are less time consuming. Desired compliance with fraud prevention requirements and the wish to avoid prosecution is pushing companies to source technological solutions that will ease the increasing burden of their risk management processes.

Robinson: The use of fraud analytics and forensic data analytics tools to proactively detect, prevent and control fraud is definitely on the rise. These tools can profile and analyse financial and non-financial data across various areas and disparate systems to find anomalous relationships, transactions or unusual patterns. They can also be used to detect fraudulent issues and raise red flags by performing tests that can identify and isolate suspicious transactions. According to an Association of Certified Fraud Examiners (ACFE) report, 38 percent of organisations increased their budget for anti-fraud technology in 2021, making this the most common area for increased investment within anti-fraud programmes. More than 60 percent of organisations in Asia-Pacific said they experienced fraud and corruption in the past two years, and senior management had increased spending on combatting fraud and economic crime, investing in advanced technologies and data analytics tools.

Foley: The use of technology, including data analytics, has become a compliance and risk management differentiator for companies. Technology can support real time transactional monitoring and provide predictive learning and intelligence that can identify fraudulent patterns and enable an organisation to promptly respond to possible misconduct. One of the main advantages of using data analytics to assist with fraud detection relates to the large amount of data that can be analysed at once, as well as the ability to merge and compare data from disparate systems. It is important to note, however, that while technology and data analytics are important tools to leverage for fraud risk management, it remains important that any 'red flags' or anomalies identified through analytics are followed up on by skilled

individuals with the requisite experience to assess whether a fraudulent transaction has occurred.

Debnath: Regulators in the UK and US now expect companies to be able to demonstrate the effectiveness of their compliance programme through metrics. This means having the analytics tools to perform real-time mining of data from compliance concern helpline management systems, employee surveys, training completion records, management communication, and so on. In the financial services sector, it is industry practice to monitor employees' business communications as part of a fraud and financial crime mitigation programme. Corporates are bringing in-house the technical ability to use technology and data analytics is such ways.

Marwood: The role of advanced data analytics in preventing and detecting fraud has increased significantly in recent years as organisations invest more in their technological capabilities. Some good examples of this are where internal and external audits are deploying software which enables review of 100 percent of a population of transactions, as opposed to a sampling approach. Forensic data analytics tools now use automation, machine learning and AI to review whole populations of data for anomalies, rather than relying on a rules-based system of tests which may be prone to human bias, and often return unworkable levels of 'false positives'. Companies are becoming increasingly interested in using these technologies as they recognise that there can be significant recoveries available as a result of analysis.

FW: How important is it to train staff to identify and report potentially fraudulent activity? In your experience, do companies pay enough attention to employee education?

Foley: Investing the right focus on training can help prevent fraud. An effective fraud awareness training programme, which includes basic information focused on what fraud is, who could commit fraud, and how fraud is committed, helps employees to identify when something does not appear right. As part of employee training, it is important to avoid discussing fraud in generalities. Instead, companies must provide specific examples to employees so that they can be aware of what fraud looks like and how they can prevent it. When developing training content, companies should focus on including examples of fraud risks that are relevant to the industry within which the company operates, so that employees can appreciate specific risks affecting the organisation. Lastly, companies have always valued the importance of employee training. However, as important as it is to push training broadly across an organisation, it is critical for a company to complement and supplement any training assignments with targeted in-person or virtual training or working sessions that include smaller groups of stakeholders. These types of training sessions give companies the ability to drill down on specific risks they may encounter given their roles, responsibilities or location.

Debnath: It is vitally important to train employees on their duty to identify misconduct and to respond properly by reporting it within the company. The key is to give employees the confidence to speak up, even if it is just a mere doubt rather than a hard evidence-based belief, without fear of being retaliated against. Employees must also know about the number of ways to report concerns, such as speaking to line managers or legal and compliance, or through the compliance reporting tools that are available. The way training is delivered has of course changed due to the COVID-19 pandemic, with traditional face-to-face training largely not possible. Even without the impact of the pandemic there is much to be said for more innovative and engaging ways to deliver essential training, such as short interactive videos or microlearnings. Training should be reinforced by regular communications from leaders and line managers.

> "THE USE OF FRAUD ANALYTICS AND FORENSIC DATA ANALYTICS TOOLS TO PROACTIVELY DETECT, PREVENT AND CONTROL FRAUD IS DEFINITELY ON THE RISE."
>
> NICK ROBINSON
> Ankura

Marwood: The culture of an organisation is one of its strongest fraud prevention tools. Being able to talk openly about what is considered 'fraud', where fraud risks arise and the expectations that the organisation has of staff, all help to maximise the chance of potential misconduct being spotted, challenged and resolved. Cultures which are closed, secretive or blame-based – where mistakes are punished – are often ones where fraud thrives. We see most organisations setting out their core expectations to new joiners

within a code of conduct, often alongside fraud and whistleblowing policies. These messages are often reiterated in periodic communications. Less common are the more sophisticated education programmes that are driven by fraud risk assessments which identify specific profiles of staff who would benefit from enhanced counter-fraud training – for example, those who engage with public officials and are at risk of exposing the organisation to bribery.

Robinson: Staff training is a huge piece of the puzzle. According to the ACFE 2020 'Report to the Nations', 43 percent of fraud schemes were detected by tips, half of which came from employees. This is why attention to employee awareness has improved in recent years. Many organisations, especially corporations in mainland China with overseas headquarters, provide anti-bribery and corruption, anti-fraud and other compliance training to staff – not only when they are newly on board, but also via periodic training to update all employees on changing laws, regulations and policies. In Hong Kong's financial institutions, financial crime compliance training, which includes anti-money laundering, counter-financing of terrorism and sanctions, is delivered to all employees by compliance officers or with the assistance of external consultants. That said, staff training is an area where organisations can always do more.

Hartley: Staff are the key drivers in any business, and it is very important to train staff to identify and report potentially fraudulent activity. Regardless of the requirement to have reasonable procedures in place from a corporate criminal liability perspective, any business should be keen to identify attempted fraudulent behaviours. One of the easiest ways to do this is through regular training and of course communication. Identifying the most common forms of fraud, such as suspicious emails, false invoices and possible social engineering, are all possible through training. The amount and types of training on offer should be proportionate to the size of the business and the type of area it operates in.

> IT IS NOW EXPECTED BY REGULATORS THAT COMPLIANCE PROGRAMMES ARE NOT ONLY EFFECTIVE BUT CAN BE DEMONSTRATED THROUGH DATA TO BE EFFECTIVE.
>
> TAPAN DEBNATH
> ABB

Sikellis: Training is critical to establishing a culture in which people will speak up and to ensure that compliance policies are embedded across the company. Trainings should be relevant and designed to foster knowledge and application through engaging, scenario-based training that brings policy content to life through real-life cases that associates can relate to and apply in their role. The culture of the company must also enable associates to raise concerns of misconduct without fear of retribution and retaliation. The process of raising allegations should be a component of all strong compliance programmes, including as an element of the training curriculum.

FW: When suspicions of fraud arise within a firm, what steps should be taken to evaluate and resolve the potential problem?

Robinson: When suspicions of fraud arise, we recommend that companies undertake the following. First, establish one version of truth. Interview all relevant personnel and assess any immediate evidence to determine: Is this unsubstantiated rumour or actual fraud? Who are the parties involved? How much money is involved? Does our in-house compliance function have sufficient capabilities to investigate further, or do we need to call in external professionals? Second, gather the evidence. This is likely to involve a document review, interviews, data analysis and e-discovery. Assign ownership of the fact-finding mission, set communication checkpoints and deadlines. Assess whether a remote investigation is possible or, if not, put in safety protocols for a face-to-face investigation. Third, decide how to respond. Do you need to restate any fraudulent accounts? Should you begin legal proceedings? Is compensation required for affected stakeholders like customers? Can you recover assets from the defrauders? Engaging neutral, external experts can often help to determine the best course of action. Finally, conduct root cause analysis. Feed the lessons learned into your fraud prevention mechanisms.

Marwood: The first challenge faced by an organisation is to ensure that all fraud suspicions are raised to suitable personnel in order to determine an appropriate response. Clarity regarding escalation channels and reporting requirements helps achieve this. Once raised, it is important that an appropriately scoped, independent review of the concern is undertaken by competent individuals. There are common failings in this regard, for example when staff without financial training are tasked with looking into accounting issues, or

when business unit leaders set the scope of an investigation occurring within their own business unit. In certain cases, for example where the board requires an independent review, it will be necessary to appoint independent forensic investigators and legal counsel in order to provide external stakeholders, including regulators, shareholders and external auditors, with sufficient comfort that fraud concerns have been fully looked into and that appropriate disciplinary and remedial steps have been taken.

Debnath: If a company finds itself in the unfortunate position of having to respond to an allegation of fraud, it has to understand what has happened. This requires the facts to be gathered as fully and as quickly as possible, either internally or with support of its external advisers. Once the facts have been established, the company should evaluate what those facts amount to: has there been a potential violation of law – 'potential' because it may dispute liability? The company should then decide whether it should self-report, to whom it self-reports, as numerous international authorities could have jurisdiction over the matter, and how to manage shareholders, the board and publicity – to name a few fundamental considerations. Instead of, or in addition to, a violation of law, the facts could indicate a breach of the company's code of conduct or policy. Remediating internal violations, whether by disciplinary action, strengthening of internal controls and processes, training and awareness, or termination of third-party relationships, will require coordination with relevant functions such as compliance, HR, procurement, internal control, audit and the business.

Hartley: Regulated firms should have clearly defined steps to follow when suspicions of fraud arise. Providing adequate training to staff on how to identify fraud and who they need to report it to is essential. Businesses regulated by the UK's Money Laundering Regulations 2007 must appoint a nominated officer to monitor suspicious activity and report it when necessary. SARs must be reported to the nominated officer by employees and evaluated to determine whether there is any evidence of money laundering or terrorist financing. A failure to report such activity to the nominated officer may itself be an offence, and so again the training for staff is an essential element. A SAR will then need to be completed and submitted to the NCA. It can be deemed an offence under the Proceeds of Crime Act 2002 if a nominated officer in the regulated sector fails to act appropriately when there is evidence of money laundering or terrorist financing. However, even in a non-regulated sector, many firms and their employees do not necessarily appreciate that they too may be committing an offence if they fail to report knowledge or suspicion of money laundering.

Sikellis: The process really begins well before an issue arises, through having a 'speak up' culture and an effective process for identifying and prioritising potentially significant matters. It is important to have an effective case triage process to focus management oversight and investigative resources on potentially high-risk matters. No doubt, a company must ensure that its investigators have an appropriate skillset to ascertain critical facts in a thoughtful, non-accusatory, yet effective manner. This approach will enhance a culture of cooperation and confidence in the objectivity of the process. In addition, once the factual background has been established, a meaningful resolution should consider the root cause of an issue and potential remediation when there is serious and substantiated misconduct. Finally, having a robust system for documenting and cataloguing the investigation and its outcome is critical.

Foley: A company should unequivocally communicate that fraud is unacceptable in all aspects of its operations, regardless of industry and business model complexity. Allegations of fraud should be taken seriously and be promptly referred and responded to by internal resources that have the capability and expertise to initiate and perform a thorough investigation, identify appropriate remediation measures, and help ensure that fraud is mitigated going forward with enhanced controls and other compliance measures, such as increased training for employees in 'gatekeeper' roles and communication around the negative impact fraud has on an organisation's corporate reputation and bottom line. Capture trends and important insights from investigations into allegations of fraud can help support continuous improvement opportunities and enhance internal controls and processes that prevent fraud and misconduct.

FW: Looking ahead, will there be greater pressure on companies to enhance their measures to mitigate potential fraud in the coming months and years? What are the potential consequences for those that fall short?

Marwood: We see an increasing focus on directors' responsibilities to respond to fraud risk, driven by greater stakeholder expectations and a regulatory desire to build confidence across the corporate environment. In the UK, for example, the recent governmental Business, Energy and Industrial Strategy (BEIS) consultation into 'restoring trust in audit and corporate governance' indicates that directors of 'public interest entities', which may include large private businesses, will be required to report on the steps they have taken to prevent and detect material fraud. In turn, external auditors will be required to audit this and to assess the effectiveness of relevant counter-fraud controls at the company. Organisations will be held to account for their counter-fraud activities by a range of stakeholders, not least employees and customers. Failure to measure up may result in lost revenue, talent and future investment, as well as potential personal sanctions for company directors, such as fines, disqualification or even criminal prosecution.

Debnath: It is now expected by regulators that compliance programmes are not only effective but can be demonstrated through data to be effective. Simply put, the potential consequences of falling short

in this regard is that when something goes wrong, such as bad actor employees or third parties engaging in criminal financial misconduct, the company is also likely to be held accountable because it did not have adequate preventative measures in place.

Hartley: Year after year, pressure grows as the burden on companies to enhance their measures to mitigate potential fraud increases. An individual as well as a company can potentially be prosecuted if they fail to prevent fraud. Given the significant increases in reports being made to the NCA, there is already pressure on businesses to mitigate their position and even adopt an 'if in doubt report it' culture. The UK's Law Commission is currently seeking views on extending corporate criminal liability as concern has increased surrounding the law in this area falling short when being applied to large corporations. While this will be welcome news in many areas, it will place a further burden on those entities already heavily regulated in the financial sector. If this becomes law, there will be wider corporate responsibility and adequate tools will need to be applied by corporations to support this.

Sikellis: No compliance programme will ever be able to detect and prevent 100 percent of potential misconduct. Nevertheless, large multinational organisations that work in a highly regulated industry like pharmaceuticals are expected to be able to ascertain and address misconduct, to ensure the integrity of their business and to meet the rapidly evolving expectations of society. Importantly, companies are expected to have zero tolerance for misconduct and thus to react appropriately when issues arise. For this reason, companies that have the ability and agility to effectively leverage resources – including in fields such as data and decision science – to identify cues and signals, will benefit by being able to ensure that misconduct is more likely to be identified and that employees are enabled to take better, more ethical decisions and actions. An inability to use such tools may result in significant gaps in knowledge that could ultimately lead to problems resulting in enforcement by regulators, large penalties and reputational damage that could be enduring.

Foley: Companies should consistently evaluate, improve and enhance their processes, training, communication and investigation practices to address fraud risk irrespective of the level of enforcement by regulators. In addition to maintaining agile compliance and fraud risk management programmes, revisiting the organisation's risk profile – typically, on an annual basis and more frequently as the regulatory landscape evolves – will identify new and emerging risks, as well as reconfirm that legacy risks remain relevant to the company's operations. Addressing corporate fraud and misconduct will remain a priority for regulators across the globe. And, given that many regulatory bodies – such as those in the US and UK – have communicated expectations for effective risk management by companies, there is an established expectation that companies be positioned to address fraud risk through a robust compliance programme.

Robinson: New hybrid workforces are increasing fraud risk for a host of reasons. Loyalty can fall away when people work remotely for long periods of time. Disengaged people find it easier to justify unethical behaviour. The use of personal devices, WiFi connections and mobile data plans can mean conventional security controls are no longer fit for purpose. Combine that situation with the financial pressure put on families from ongoing uncertainty and economic downturns, and suddenly you have both the motive and opportunity for fraud. Organisations that do not take this threat seriously will suffer the triple whammy of fraud consequences: loss of data, finances or both. There is also an accompanying reputational hit, as well as financial penalties imposed by regulators or other authorities. In the current environment, few companies are capable of taking these hits in their stride. Those in economic distress are more vulnerable to bearing the cost of fraud. ■