REPRINT

FINANCIER WORLDWIDE MAGAZINE

ROUNDTABLE

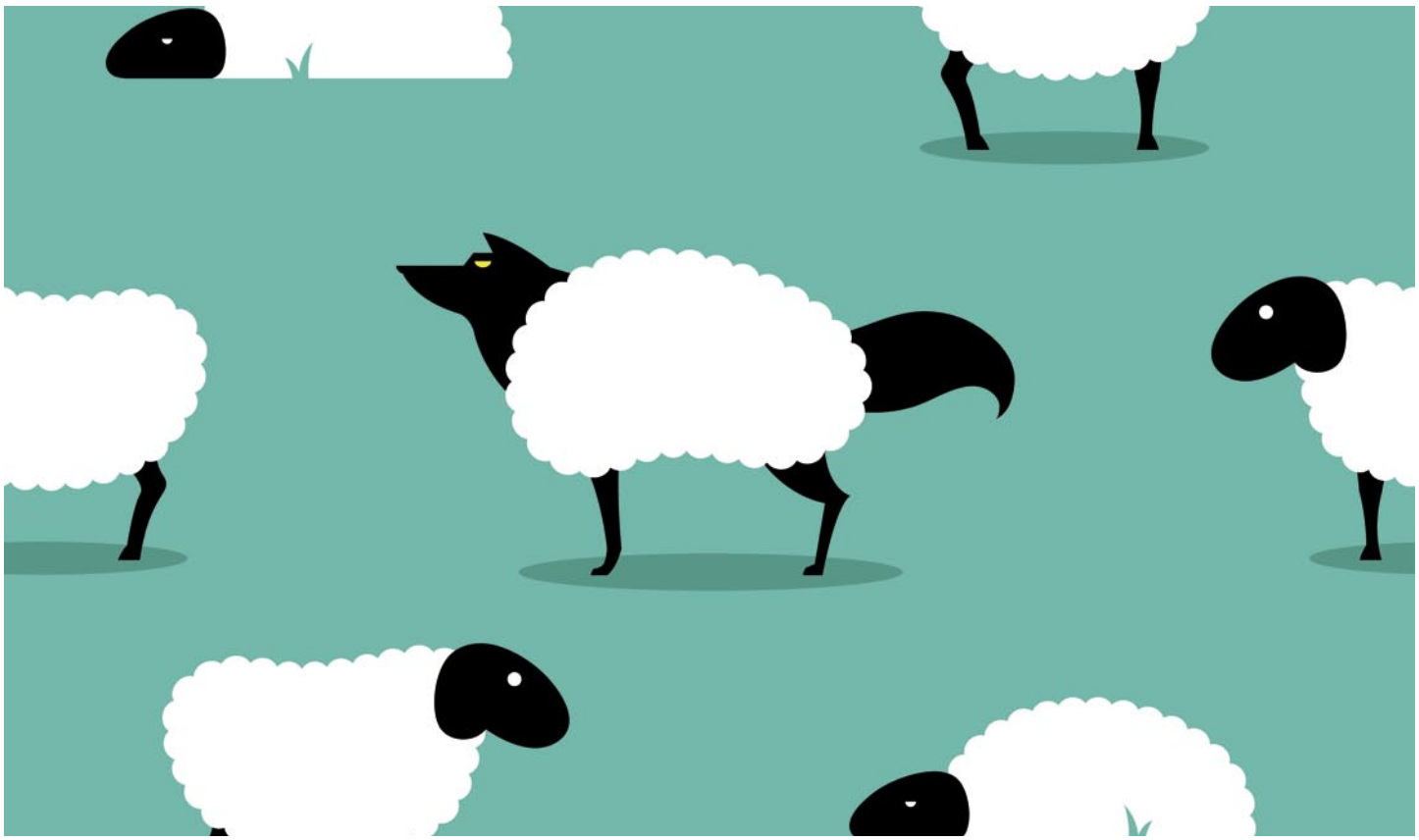
Corporate fraud

REPRINTED FROM
NOVEMBER 2018 ISSUE

FINANCIER WORLDWIDE corporatefinanceintelligence

www.financierworldwide.com

ROUNDTABLE:
CORPORATE FRAUD



Corporate fraud is a global scourge costing hundreds of billions per annum. Asset misappropriation, money laundering, insider trading, cyber attacks and general business misconduct are among the most frequently reported crimes, particularly by financial institutions. Inadequate anti-fraud systems compound such activity, meaning clear red flags are often missed due to a lack of robust policies and procedures. Disturbingly, with technology and globalisation continuing to advance, the opportunity for corporate fraud is likely to grow. ■

THE PANELLISTS

Jane Colston
Partner, Brown Rudnick LLP
T: +44 (0)20 7851 6059
E: jcolston@brownrudnick.com
www.brownrudnick.com

Jane Colston is one of the award-winning 14 litigation partner team at Brown Rudnick London, combining cross-border civil fraud, criminal and regulatory experience under one roof. She has acted in numerous complex, cross-border fraud cases and has extensive experience of forensic investigations. She has also managed numerous cases involving freezing, search, disclosure, gagging and delivery up injunctions.

David Pasewaldt
Counsel, Clifford Chance Deutschland LLP
T: +49 69 7199 1453
E: david.pasewaldt@cliffordchance.com
www.cliffordchance.com

David Pasewaldt, LL.M., advises national and international companies in the field of white-collar crime and compliance. He specialises in conducting internal investigations, defending companies in investigation proceedings and the prevention of criminal risks. Dr Pasewaldt regularly publishes articles in professional journals and gives lectures on white-collar crime. He is a lecturer at the Frankfurt School of Finance & Management.

Adrian D. Mebane
Deputy General Counsel and VP, Global Commercial & Supply Chain, The Hershey Company
T: +1 (717) 534 7673
E: amebane@hersheys.com
www.hersheys.com

Adrian Mebane is vice president and deputy general counsel for The Hershey Company. Leading the company's global legal risk centre of excellence, he is responsible for addressing high impact risks in the global ethics and compliance, regulatory, litigation and intellectual property practice areas. Mr Mebane also works collaboratively with, and is a trusted adviser to, executive leadership, senior management, the audit and finance and risk management committees and the board of directors.

James A. Garrett
Vice President & Chief Risk and Compliance Officer, NuVasive, Inc
T: +1 (858) 320 4554
E: jgarrett@nuvasive.com
www.nuvasive.com

James A. Garrett serves as vice president and chief risk & compliance officer at NuVasive, Inc. He oversees global compliance, risk management and information governance, and also serves as the company's chief privacy officer. As the leader of the company's global risk & integrity (GRI) department, he chairs the company's corporate risk management committee and corporate integrity steering committee.

Hannah Laming
Partner, Peters & Peters Solicitors LLP
T: +44 (0)20 7822 7752
E: hlaming@petersandpeters.com
www.petersandpeters.com

Hannah Laming is a partner with significant expertise in business crime. She advises on serious fraud, corruption, private prosecutions, internal investigations, Financial Conduct Authority (FCA) regulatory issues (civil and criminal) and economic sanctions. She also advises firms and individuals on insider dealing, market abuse, unauthorised trading, financial promotions, systems and controls breaches, and investigations into the conduct of regulated individuals, including those with significant influence functions.

Nicholas S. Goldin
Partner, Simpson Thacher & Bartlett LLP
T: +1 (212) 455 3685
E: ngoldin@stblaw.com
www.stblaw.com

A former US federal prosecutor and co-chair of Simpson Thacher's privacy and cyber security practice, Nick Goldin handles cyber incident response, white-collar and regulatory defence and internal investigations, and provides ongoing corporate compliance advice. Based in New York, Mr Goldin is recognised in Chambers as "incredibly insightful", "highly responsive" and "able to connect the dots probably better than any other attorney". He was named a 2018 BTI Client Service All-Star for "delivering the absolute best client service".

Aisling O'Shea
Special Counsel, Sullivan & Cromwell LLP
T: +1 (202) 956 7500
E: osheaa@sullcrom.com
www.sullcrom.com

Aisling O'Shea is special counsel in Sullivan & Cromwell LLP's Litigation Group. She focuses her practice on criminal defence, government investigations and the Foreign Corrupt Practices Act (FCPA). Before joining Sullivan & Cromwell as an associate working on complex financial investigations, Ms O'Shea spent five years as a trial attorney in the fraud section of the US Department of Justice's (DOJ) criminal division. Within the fraud section, she was a member of the FCPA unit.

FW: Could you provide an overview of the types of corporate fraud currently permeating the financial world? What social and economic trends seem to be driving fraudulent activity?

Colston: According to the BBC, in the UK, £145m was lost in the first half of 2018 to fraudsters, through the hacking of email accounts and phishing scams. That amounts to a huge number of accounts banks are allowing to be opened which are then used to receive and launder stolen monies. Often, civil disclosure orders against banks will reveal that the banks' anti-money laundering (AML) systems are woefully inadequate. Often, banks are not spotting clear red flags and halting money transfers.

Garrett: The breadth and scope of cyber crimes is the most significant trend facing all industries, as fraud schemes, the opportunities for fraud, as well as the sophistication of those perpetuating the fraud, continue to increase at an alarming rate, as does the number of fraudsters. Social changes and generational differences in how we view information and privacy are exacerbating the potential and opportunity for fraud, as are technological advances and globalisation.

O'Shea: Our increasingly global economy means there are more opportunities for business that bring with them new areas for potential fraud risk, such as operating in countries and within different legal and cultural paradigms than those in which a company is experienced and has already developed effective risk management programmes. More specifically, the dramatic and ever-changing impact of technology as a social and economic trend has led to a significant new frontier of fraud risk, particularly for financial institutions.

Laming: Consumer fraud, asset misappropriation, cyber crime and business misconduct are the most frequently reported fraud and economic crimes across the financial services industry, according to the latest PwC Global Economic Crime and Fraud Survey 2018. The survey highlighted that most frauds are committed by internal actors, such as senior management and rogue employees, who are a third more likely than external actors to be the perpetrators of the most disruptive frauds. While cyber crime, mostly malware and phishing, has increased recently, asset misappropriation, be it embezzlement or false accounting, continues to be prevalent. Business misconduct such as money laundering, bribery and currency manipulation also continues to make headlines.

Pasewaldt: The types of corporate fraud evident today are more multifaceted than ever before. Though embezzlement, false accounting, tax evasion and market manipulation have long been known as typical examples of corporate fraud in the financial sector, the emergence of globalisation and new technologies have changed the face of corporate fraud. Recent, relevant examples include the alleged manipulation of benchmark interest rates such as Libor and Eurobor and the so-called 'cum/ex transactions' – tax-evasion schemes involving large-volume cross-border share transactions around the dividend date that lead to multiple refunds of a withholding tax that has only been paid once. At the same time, the financial industry is facing the threat of cyber attacks and intellectual property theft, both of which have been enhanced by the increased digitalisation of large parts of the industry.

Goldin: We have seen a steady stream of corruption, cyber fraud and insider trading activity for a number of years, and the trend shows little sign of slowing. If there has been any slowdown in accounting scandals, some would say that is because the economy has been roaring, and that it is more likely when conditions are bad that rogue employees will resort to gimmicks and deception to hit their numbers. The other development has been the increasingly cross-border nature of many types of investigations beyond corruption – from the currency benchmark investigations that began a number of years ago to the more recent money laundering, data breach and international sanctions inquiries. The rise of cross-border misconduct means more complex investigations being conducted by more regulators in more jurisdictions.

Mebane: Many types of fraud impact global corporations, including corruption, money laundering, misappropriation of assets and falsification of financial information, to highlight just a few. Although the methods from which fraudulent behaviours are derived have not changed, the complexity of these activities has increased because of modernised technology and the globalisation of companies' business operations. As a result, senior leaders and boards of directors are increasing their attention to the causes, identification, prevention and remediation of corporate fraud concerns affecting their operations. The implications of companies not becoming acutely focused on these matters may have severe impacts from legal, compliance and reputational standpoints, as corporate fraud can affect all aspects of an entity's business operations.

FW: How would you characterise the impact of legislation and regulation on corporate efforts to mitigate and manage fraud? To what extent have companies tailored their governance and control procedures to accommodate tighter regulatory scrutiny?

Garrett: Legislation and regulation are extremely slow to mitigate the risk of cyber fraud, as are regulators and law enforcement. State-sponsored cyber threats get all the headlines – for example Russia and China – but for the majority of corporations, the threat is likely more real from its own employees or a single hacker working on a home computer. In other words, most companies are not at risk of corporate espionage, but any company can be held ransom for $30,000 if their billing or payroll software is compromised. Given the volume of these types of cases, federal authorities often do not take a serious interest and local authorities do not have the jurisdiction or resources to effectively take action. Accordingly, in addition to upgrading their information security platforms with systems, tools and teams of analysts, many companies are working to strengthen their employee training and awareness because cyber fraud can occur at any level of the organisation and in any department or division.

O'Shea: More sophisticated companies are always examining legal and regulatory developments to ensure that their internal controls are keeping pace with such developments, particularly in areas where there appears to be tighter regulatory scrutiny. Interestingly, there has been a trend over the past few years of corporate fraud cases involving activities that have not been historically subject to tight or specific regulation. In light of this trend, many companies are taking a wider view of control procedures to further develop enhanced controls for what have traditionally been non-regulated activities. Whereas in the past many companies may have felt comfortable tailoring their controls to the existing regulatory regime, increasingly there is a more organic approach being taken to internal controls so that they are not primarily focused on regulations, but on all areas that present key risks.

Pasewaldt: The recent implementation of tighter legislation and regulatory frameworks in almost every relevant jurisdiction has imposed stricter requirements on companies from the financial sector to mitigate and manage corporate fraud. Apart from, for example, the increase of monetary penalties for violations of capital market laws that were introduced in the European Union following a harmonisation, the various tightening of national AML laws due to relevant provisions under EU regulations has forced financial institutions and investors to adapt their control procedures and governance accordingly. In Germany, the latest amendment of the German Money Laundering Act expanded the obligations of relevant companies and, at the same time, increased the regulatory and investigative powers of the German Federal Financial Supervisory Authority, which is already making use of these additional powers in practice.

Goldin: With the heightened regulatory expectations in the corporate fraud space, many companies have redoubled their efforts to deter and identify financial crimes and other wrongdoing. The message that the international authorities have tried to express through the staggering corporate fraud settlements of recent years has been clear: companies that take robust steps to foster a strong culture of compliance and that respond to suspected wrongdoing with comprehensive, objective inquiries and then voluntarily self-report, will feel less pain than those that do not. Whether, in practice, the magnitude of the leniency actually granted in settlements is sufficient to incentivise companies to take all of these steps in every instance is, in many quarters, still an open question.

Laming: The focus of recent legislation and regulation has predominantly been on money laundering, terrorist financing and bribery and corruption. The UK Bribery Act (UKBA) has had the biggest impact in terms of prompting firms to increase their compliance efforts and tighten their policies. The majority of organisations have reviewed and revised their policies and procedures with a view to preventing bribes being paid on behalf of the company. However, the introduction of further 'failure to prevent' offences should be approached with caution as they may not have the same positive impact as the UKBA.

Mebane: The impact of legislation and regulation on a company's efforts to identify, mitigate and manage fraud can be a 'moving target' because of the frequent changes and updates to legislation implemented by both international and local regulators within the markets that a company may operate. Consequently, robust employee training and fraud awareness through frequent communication is vital to preventing misconduct. As a complement to enhanced training and communication, many corporations are leveraging data analytics and other forms of technology to help identify potential gaps and areas of heightened vulnerability. To effectively identify and manage fraud, it is imperative for a company to take a risk-based approach. Undertaking such an approach helps to ensure that an organisation's governance and control procedures address risks specific to its operating model and strategic priorities.

Colston: Banks often refuse to compensate the target of transfer fraud or push payment fraud if the victim authorised the mistaken payment. A draft voluntary code for banks has recently been published, under which, if customers take 'the requisite level of care' they should be reimbursed by their bank if defrauded. This will involve the customer showing that they have, for example, taken reasonable steps to confirm the payee and were not grossly negligent. A final code

> "INTERESTINGLY, THERE HAS BEEN A TREND OVER THE PAST FEW YEARS OF CORPORATE FRAUD CASES INVOLVING ACTIVITIES THAT HAVE NOT BEEN HISTORICALLY SUBJECT TO TIGHT OR SPECIFIC REGULATION."
>
> AISLING O'SHEA
> Sullivan & Cromwell LLP

should be in place in early 2019 and five banks are reported to have already adopted the code. Such a code will clearly incentivise banks to beef up their AML and artificial intelligence (AI) systems to detect unusual behaviour and prevent fraud. Banks should also ensure that the sort code, account number and account name all tally, as fraudsters know, at present, banks only check the sort code and account number.

> "WITH THE HEIGHTENED REGULATORY EXPECTATIONS IN THE CORPORATE FRAUD SPACE, MANY COMPANIES HAVE REDOUBLED THEIR EFFORTS TO DETER AND IDENTIFY FINANCIAL CRIMES AND OTHER WRONGDOING."
>
> NICHOLAS S. GOLDIN
> Simpson Thacher & Bartlett LLP

FW: Which corporate fraud cases have gained your attention in recent times? What do these cases tell us about the extent of the threat facing the corporate world?

Goldin: Two recent matters are particularly noteworthy. The first is the settlement relating to the massive data breach at Yahoo!, where the US Securities and Exchange Commission (SEC) charged the company for failing to disclose information about the data breach until almost two years after the incident. The second stemmed from a tweet by the chief executive of Tesla concerning plans to take Tesla private. As part of a settlement with the SEC, Tesla agreed to enhance its disclosure controls designed to ensure that information disseminated to the market is accurate and timely. The takeaway is clear: while the government remains focused on the accuracy of corporate disclosures to the market, it is also scrutinising the timing of those disclosures as well as a company's disclosure controls and procedures.

Pasewaldt: A number of corporate fraud cases have caught the public's attention in Germany in recent years. Following alleged tax evasion by way of so-called 'VAT carousels' and the cum/ex transaction schemes that allegedly led to considerable damage for the German treasury, the German car manufacturing industry is currently facing allegations of, and large-scale investigation proceedings into, alleged manipulation of exhaust fumes from diesel engines. At the same time, German companies are being increasingly exposed to cyber attacks and intellectual property theft, both of which can have devastating consequences for the business targeted. This development shows that continuing digitalisation requires control measures beyond the usual prevention measures, namely a solid cyber security plan and the implementation of relevant measures.

Laming: Few corporate fraud cases make their way to the criminal court as these cases are notoriously complex and resource-intensive to investigate and prosecute – the standard of proof is higher than in civil trials and there are extensive disclosure obligations on the prosecutor. Limited resources have necessarily resulted in the prioritisation of other types of offending, such as terrorism, violent crime and sex abuse cases. As a result, firms and high-net worth individuals, who find themselves the victim of fraud, are increasingly bringing private prosecutions against the perpetrators, in addition to their civil recovery proceedings, as an alternative form of redress, and these cases are gaining traction. In June 2018, a director was sentenced in the UK to eight years' imprisonment – his co-conspirator got 14 years in a separate trial – following a private prosecution brought by a large shipping firm for defrauding the firm of over €100m.

Mebane: One of the first corporate fraud cases that comes to mind is Wells Fargo, a bank that became embroiled in a fake accounts scandal when employees were trying to meet certain quotas. The bank was fined $1bn earlier this year. Not only was the underlying misconduct egregious, the way in which Wells Fargo handled these matters when reported to the company was equally concerning because it failed to conduct appropriate and timely investigations into the allegations. Another example is the matter involving Theranos, a technology corporation that strived to evolve the 'world of medicine' through advanced technology that was ultimately not Theranos'. In the process, the company gained support from key individual and corporate investors. As a result, the SEC charged Theranos with fraudulently creating more than $700m in external investments. The matter settled with the SEC and Theranos agreed to pay a $500,000 fine and turn over 19 million shares.

Garrett: The Wells Fargo case is the most interesting major corporate fraud case we have seen in a long time. It is interesting because it involved, among other things, an 'indirect' inducement or incentive for the fraud to occur. Unlike Enron, where there was more of a direct 'scheme' to commit illegal acts or fraud, Wells Fargo set up an aggressive incentive scheme that led others in the organisation to commit misconduct by opening up fraudulent accounts. That is not to say that management did not intend, knowingly or recklessly, to set up the incentive plan that led to the misconduct,

but the facts are somewhat unique as compared to some of the other large corporate fraud cases we have seen in recent years.

FW: In your opinion, do boards and senior executives take a sufficiently proactive approach toward addressing the risk of fraud within their organisation?

O'Shea: There has been a shift in the amount of attention boards and senior executives have given risk issues. I think now, many senior executives and board members are even more sensitive to fraud risk and are far more likely to proactively ask questions or require additional reporting about fraud risk within the organisation and what is being done to mitigate it.

Pasewaldt: The boards and senior executives of blue chip companies and other large corporations in Germany are paying increased attention to, and dedicating more resources to, addressing corporate fraud within their organisations. In most companies, relevant controls and prevention measures are the responsibility of top-level management, and some of these companies have learned their lessons from previous experiences. This development is also accompanied by an application of stricter standards by German courts and authorities when it comes to the question of the individual liability of senior managers, specifically regarding an allegation of a violation of supervisory duties, and relevant corporate penalties.

Colston: A recent survey suggested that most internal fraud is carried out by a man in an executive role between the ages of 40 and 50. Often, the hierarchy and culture of a company means a dishonest director is not questioned. The dishonest director is frequently assisted by other directors who turn a blind eye or are bullied or rewarded into silence. Frequently, such directors are oblivious to how 'Nelsonian knowledge', turning a blind eye or neglect will not excuse their breach of fiduciary duty. Like the banks, honest directors should play a vital role in detecting and preventing fraud. Those directors who fall below the standard of care required of them should expect to be held to account for any fraud the company suffers while they were 'sleeping at the wheel' or blindly following. Loyal disagreement and active management are key to preventing fraud.

Garrett: Most members of boards of directors and senior executives, at least in public companies, take their responsibilities very seriously with regard to corporate fraud. The combination of personal liability and public exposure necessitates that most individuals in these positions, when informed of significant risk areas, act with integrity and work to prevent corporate fraud. However, not all corporate mechanisms and reporting lines lend themselves to open and transparent communication of risk areas that could lead to fraud.

Mebane: Boards of directors and senior executives have an integral role in fraud detection, management and remediation. It is these corporate leaders who guide the effectiveness of a company's response to fraud allegations. Leadership reinforces and supports an appropriate and timely investigation of the allegations, adjustments to company policies, such as codes of conduct and fraud policies, to reinforce compliance expectations in a concise manner, improved internal controls, more frequent training for employees and business partners and taking the appropriate disciplinary actions against employees and third parties that may have violated corporate policies or regulations. In an environment where regulatory activity involving corporate fraud is ever-changing, directors and senior executives should be even more vigilant in demanding and championing an operating environment where misconduct is not tolerated.

Laming: The level and nature of involvement from boards and senior executives in addressing fraud risks within their organisation differs according to the size, management structure and business activities of the organisation, as well as on the culture of the firm. In smaller organisations, boards and senior management tend to be more personally involved in the design and implementation of fraud risk measures. In larger organisations, the board may delegate fraud risk management to a board-level committee, which is tasked with reviewing and conducting risk assessments, and establishing anti-fraud programmes, controls and procedures.

Goldin: While there is no single way to fully address the risk of corporate fraud, it

> AI CAN BE A POWERFUL TOOL FOR FIRMS IN DETECTING FRAUD, PARTICULARLY WHERE IT IS USED TO IDENTIFY ANOMALOUS RELATIONSHIPS, TRANSACTIONS OR UNUSUAL PATTERNS, SUCH AS DUPLICATE SUPPLIER INVOICING.
>
> HANNAH LAMING
> Peters & Peters Solicitors LLP

is clear that senior leaders at the forefront of mitigating fraud are always thinking about ways to enhance their programmes across their enterprises. They are leading by example, retaining subject matter experts to evaluate risk and improve controls, and regularly looking for opportunities to remind the rank-and-file about how seriously the company takes compliance with the letter and spirit of the law.

FW: How would you advise companies go about setting up systems to detect potential fraud?

Pasewaldt: The cornerstone of an effective fraud management system is the risk analysis, which recognises the characteristics and peculiarities of a company, including the type of its business, specific regions in which it operates and so on. Based on such a risk analysis, which should be pursued on an ongoing basis, the company can develop and maintain customised measures to detect and prevent potential fraud. Relevant measures can include a variety of individual checks and controls, such as in the areas of bookkeeping and accounting, counterparty due diligence, an implementation of guidelines and policies, relevant training for employees, IT solutions in the course of cyber security, and others.

Garrett: Many companies have systems and tools that could help identify, manage and mitigate the risk of corporate fraud. The issue is not the systems, but the management of the culture and communications. Enron and Wells Fargo both had hypercompetitive cultures where it was expected that employees 'get it done at all costs'. This type of culture does not lend itself to open and transparent communication where corporate fraud is discouraged and uncovered. There must be a balance. Driving revenue is an imperative for all companies, but the expectation from the top about how you drive revenue is what is important. Just as important is having a culture where employees are recognised and rewarded for doing the right thing in the face of ongoing and perpetual business challenges.

> "MANY COMPANIES HAVE SYSTEMS AND TOOLS THAT COULD HELP IDENTIFY, MANAGE AND MITIGATE THE RISK OF CORPORATE FRAUD. THE ISSUE IS NOT THE SYSTEMS, BUT THE MANAGEMENT OF THE CULTURE AND COMMUNICATIONS."
>
> JAMES A. GARRETT
> NuVasive, Inc

Mebane: An effective fraud prevention programme should be risk-based and focus on the specific impacts faced by an organisation. It should consider input from various cross-functional departments, including individuals with a deep understanding of business operations and processes, compliance professionals and finance personnel to help identify, implement and maintain practical controls. Senior executives should also assume the important role facilitating the appropriate level of attention and resources – for example personnel and budget – are committed to the programme. Additionally, and to further the relevancy and effectiveness of a fraud compliance programme, controls should be integrated into business processes and complemented by written policies and procedures.

Laming: I would advise a two-pronged approach when setting up systems to detect potential fraud. First, invest in fraud detection technology. Second, invest in training staff on fraud awareness. AI can be a powerful tool for firms in detecting fraud, particularly where it is used to identify anomalous relationships, transactions or unusual patterns, such as duplicate supplier invoicing. However, it is only a part of the solution. It is important to provide fraud awareness training to all employees across the firm, educating them on what fraud is, what role they play in preventing, detecting and deterring it, what the firm's approach is to fraud risk management, and educating them on where they can seek assistance and advice.

Goldin: It is hard to pull off a well-designed, properly balanced fraud detection system without knowing your areas of risk. So, a good first step is a risk assessment that identifies corporate activities, functions and personnel that are most susceptible to fraud. Once areas of risk have been identified, a company should design and implement systems and controls that are specifically tailored to mitigate and detect fraud, while taking into account commercial considerations. And, an effective fraud prevention and detection programme requires training employees so that they understand the policies and procedures, know how to identify a suspicious transaction, and are comfortable reporting their concerns without fear of retaliation.

Colston: A sensible first approach is to ensure the segregation of duties within a company to prevent one individual having control of an end-to-end process. That has to be thoughtfully done, however, to ensure that there is visibility and oversight across the whole end-to-end process. If tasks are put into silos, it diminishes the ability of any one individual being able to identify red

flags and whistle blow, and increases the risk that key information is not passed on in time. Good team work and communication is vital.

FW: How important is it for companies to train staff to recognise and report potentially fraudulent activity within their organisation? In your experience, do companies pay enough attention to employee education and reiterating its value in this regard?

Mebane: Although a company can undertake all necessary efforts to leverage technology and data analytics, and integrate and maintain appropriate internal controls, ignoring human behaviour and how it may affect the effectiveness of fraud prevention activities is a failure for a company. Employees are the primary defence for an organisation against fraud. As a result, providing frequent and effective training on how to identify 'red flags' within the context of an employee's role at the company, as well as the mechanism for reporting these matters to the company, is of utmost importance.

Colston: Training is fundamental. However sophisticated the fraud detection checklists may be in a business, they are likely to be consigned to desk drawers unless teams buy-in to their fundamental role as a first line of defence in preventing fraud and understand why the checks are in place. Building a culture of capability is important so that relevant teams will properly scrutinise data with the fraud risk in mind. Knowing fraudsters' usual modus operandi helps staff spot it when it happens to them. Of course, such training has to emphasise that any interrogation has to be balanced so genuine users and customers are not put off by being treated as if they were potential suspects.

Laming: The technology designed to detect and prevent fraud, even when it is machine learning (ML), is only as good as the humans operating and working within it. There is a risk that, as companies spend more on the technology to combat fraud and economic crime, they may neglect employee education. Most companies provide basic online fraud and bribery training modules to employees as a standard for their induction but, of course, there is always scope for further employee education. Firms could benefit from enhanced fraud awareness courses that enable them to understand, comprehensively, the risk of fraud, be alert to red flags, understand the company's fraud risk management, and put their learning into practice, while continuously monitoring the system.

Goldin: While each element of a fraud detection programme is important, training is critical. If employees do not understand how to recognise and report potentially fraudulent activity, and if they are not comfortable doing so, the programme will suffer. While embedded fraud detection controls and procedures are important, they are just one part of a well-designed compliance programme. Employee training programmes can be a combination of in-person and online modules, and are most effective when tailored to the specific functions of the employees being trained. Increasingly, corporate leaders are appreciating not only that promoting a 'speak up' culture among employees is a critical component of a compliance programme, but that cultivating this culture takes time, effort and repetition.

Garrett: It is absolutely critical for all employees, regardless of role, to be trained on recognising and reporting fraudulent activity. However, the emphasis should be on building a culture of integrity where fraudulent activity is not accepted, hence there is no need to report it. Anonymous reporting hotlines and 'open-door' policies are absolutely necessary, but they are generally vehicles for employees to report bad acts that have already occurred and they are not used very often. Companies should spend more time highlighting the principles of integrity, honesty and fairness, rather than training people on who to call when something is not right.

O'Shea: Training is critically important. Making sure that employees who are not necessarily in control functions have the ability to recognise red flags or other signs of fraudulent activity, and feel empowered to report what they observe, is the first, and in many ways most critical, line of defence. In recent years, companies have placed an increased focus on training employees outside of control functions on legal and compliance risk, including fraud risk, and those trainings are extremely valuable for a variety of purposes – their actual educational content, instilling senses of responsibility and empowerment in employees, and demonstrating in a concrete

> "IGNORING HUMAN BEHAVIOUR AND HOW IT MAY AFFECT THE EFFECTIVENESS OF FRAUD PREVENTION ACTIVITIES IS A FAILURE FOR A COMPANY. EMPLOYEES ARE THE PRIMARY DEFENCE FOR AN ORGANISATION AGAINST FRAUD."
>
> ADRIAN D. MEBANE
> The Hershey Company

way that compliance is a core cultural value for the corporation.

Pasewaldt: Training for employees, to increase awareness of potential fraud, is a crucial element of an efficient fraud-prevention programme. Under the German administrative offences law, such training can be a required measure of disproving allegations of violations of supervisory duties against senior managers when corporate fraud was actually committed by employees within the company. This is similar to the six principles for a defence of 'adequate procedures' to disprove allegations of failure to prevent bribery under section 7 of the UKBA or the new offences in the UK of failing to prevent the criminal facilitation of tax evasion.

> "TRAINING FOR EMPLOYEES, TO INCREASE AWARENESS OF POTENTIAL FRAUD, IS A CRUCIAL ELEMENT OF AN EFFICIENT FRAUD-PREVENTION PROGRAMME."
>
> DAVID PASEWALDT
> Clifford Chance Deutschland LLP

FW: In what ways have companies changed the way they manage and respond to fraud in light of the renewed focus on encouraging and protecting whistleblowers?

Laming: Many organisations have adopted confidential whistleblower hotlines for employees to voice concerns about financial crime occurring within the organisation, and that includes potential fraud. Some regulatory laws require companies to have a whistleblower champion, such as a non-executive director, who has responsibility for overseeing the effectiveness of internal whistleblowing arrangements, including arrangements for protecting them against detrimental treatment and preparing annual reports to the board. The treatment of whistleblowers has not always been consistent throughout the industry, with some companies alleged to have fallen foul of regulatory laws for attempting to expose the identity of whistleblowers.

Goldin: Especially since the Dodd-Frank Act created a bounty programme for employees who report suspected corporate fraud to the SEC, companies have stepped up their efforts to encourage internal reporting of suspected misconduct. These efforts include greater promotion of internal reporting channels, enhanced training on identifying and reporting suspected misconduct, and renewed efforts to drive corporate anti-retaliation policies. In addition, to encourage employees to raise concerns directly to supervisors, many companies have web portals and global hotlines that accept anonymous reports. Beyond encouraging internal reporting, many companies have strengthened procedures for handling reports to ensure that the allegations are investigated and addressed by subject matter experts in a consistent and timely manner.

Mebane: Companies have adjusted the way allegations are addressed by taking all concerns seriously and initiating an investigation into them since organisations remain under increased scrutiny on how allegations are treated once received. To that end, a governance structure related to investigative processes and protection of whistleblowers should be prioritised. Employees and third parties with the courage to report a concern to a company are important resources and an organisation should implement and maintain a robust framework that strives to protect these individuals and drive an effective process for investigating and remediating allegations of fraud that are brought forward.

O'Shea: There has been a sea change in terms of internal marketing and awareness of whistleblower resources within companies. Whistleblower hotlines or their equivalent have been around for a long time at larger, more sophisticated companies, but may have suffered from a lack of internal awareness or a lack of corporate resources for meaningful follow-up. Increased public attention on encouraging and protecting whistleblowers, and an increased corporate focus on creating cultures of compliance, have led to a significant expansion of corporate resources devoted to addressing whistleblower demands and, perhaps more importantly, a considerably heightened awareness on the part of employees that such resources are available to them. Employees now seem to have a much clearer sense that there are avenues available to them to share their concerns internally, whereas in the past a company might have had a whistleblower hotline that received one call a year due to lack of internal awareness.

Pasewaldt: The clear trend in the German corporate landscape is to implement formal reporting procedures regarding suspicions of corporate fraud. This trend is accompanied by different attempts to facilitate such reporting by protecting whistleblowers. Due to the absence of both a relevant statutory regulation and uniform case law in Germany, companies are increasingly setting up whistleblower programmes that include amnesty for employees in an

attempt to encourage reporting. However, such amnesty must be limited, particularly in terms of disciplinary measures under existing labour laws. By contrast, such amnesties can never validly exempt employees from investigations, prosecution or punishment by German authorities and courts under the German criminal or administrative offences law, specifically where the reporting employee was involved in the fraudulent activity.

Garrett: There has been a renewed focus on the importance of anonymous reporting systems and anti-retaliation policies. To some extent, companies have also increased efforts with regard to building a compliant culture, but this takes time and a culture built on a shaky foundation is unlikely to change. In the short term, many companies have resorted to an increased focus on the human resources (HR) function to create a positive work environment in the hope that it will reduce the likelihood of a whistleblower. HR can play a role in driving positive change in this regard, but the emphasis on integrity needs to come from senior management and all managers and employees need to be held accountable to meeting those standards.

FW: In terms of third-party relationships, can you highlight the main fraud-related risks that companies face? What measure can be taken to strengthen supply chain processes – a significant source of fraudulent activity?

Goldin: Among the greatest risks relating to third parties is that an employee of the company will collaborate with the third party to engage in misconduct in some form. While the use of vendors and agents to bribe government officials often receives the most attention, third parties can be used to facilitate commercial bribery, employee defalcation and various other forms of fraud. Some of the most effective ways to mitigate third-party risk are adopting comprehensive policies and procedures for onboarding third parties, and implementing rigorous controls for paying third parties. Provisions in agreements with third parties allowing for periodic monitoring and auditing of the third party are also increasingly common.

Garrett: The risk of fraud is always higher when engaging third parties, particularly in countries with a history of corruption or a culture where business creates the opportunity for fraud and corruption, such as where gifts are the norm. Vendor due diligence is key to mitigating corruption risk, as is good contracting, but effective mitigation requires ongoing oversight of key third parties, regardless of whether they are in the supply chain or if they support other business units like regulatory, sales or marketing. As such, contracts with third parties should, to the extent possible, permit compliance training, monitoring and auditing.

Mebane: When not managed appropriately, third parties could become a significant organisational risk. It is important that a company not only establish procurement and sourcing procedures that deliver quality and effective cost control measures, but also understand with whom they are conducting business. This can be accomplished through a due diligence programme established to identify risks specific to the company, as well as potential concerns involving the third parties' prior or ongoing commercial activities and how its operating model could expose the company to undue risk and fraud. The due diligence process can also be leveraged as a tool for the company to highlight and reinforce its compliance expectations with the third party.

Pasewaldt: Third-party relationships can expose companies to a variety of fraud-related risks. The nature and scope of such risks also depends on the definition of corporate fraud. Based on a broad understanding, apart from the traditional risk, such as fraud, the theft of trade and business secrets or know-how, third-party relationships can bear risks of tax evasion schemes, such as where a financial institution is involved in a relevant scheme by way of stock trading, bribery and corruption, for example where a company engages sales agents or other intermediaries to facilitate its business or money laundering. Against this background, a thorough risk assessment and third-party due diligence are crucial to tackling risks of corporate fraud, also when it comes to supply chain processes.

Colston: Invoice fraud is prevalent, with criminals researching suppliers to large corporations by reviewing publicly available information. The fraudster will then communicate with the supplier to phish for information about the supplier – for example, perhaps they call to check

> "INVOICE FRAUD IS PREVALENT, WITH CRIMINALS RESEARCHING SUPPLIERS TO LARGE CORPORATIONS BY REVIEWING PUBLICLY AVAILABLE INFORMATION."
>
> JANE COLSTON
> Brown Rudnick LLP

a postcode, thereby seeking to establish an impression that they work for the end customer, so that when they subsequently call seeking more sensitive information it is provided. With this confidential information, the target company is approached and conned into paying the fraudsters in the mistaken belief they are paying the supplier. Teams responsible for invoicing customers or paying suppliers should be trained to look out for red flags, such as email change requests at the same time as bank account changes, copy letterheads or bank stamps or emails from senior people writing administrative letters at large corporations. There should be a culture where suspicions are acted on and reasonable enquiries made before any payments are authorised. Picking up the phone to the supplier or receiving party to check their bank account details when a bank account change email has been received purporting to be from them is a sensible and fast way to check that all is above board. That requires staff on the ground to be empowered to take ownership and act in the face of suspicions.

Laming: Companies may unknowingly become embroiled in financial crimes like fraud, bribery, money laundering or breaching sanctions through the actions of their third parties, including suppliers and agents. The UKBA makes a firm vicariously liable for those who pay bribes on its behalf if it does not have adequate procedures in place to prevent this happening. Companies should ensure that they have undertaken proper due diligence on third parties involved in their business, particularly if they are located in a high-risk jurisdiction or work in high-risk sectors, such as oil and gas.

FW: What advice would you give companies on how to respond to an allegation of fraud within their ranks or across their supply chains? How should a company's overall goals and objectives be incorporated into the fraud investigation process?

Colston: When fraud is suspected or uncovered, prompt and focused action is a first essential step. Information about the suspected fraud should be limited to a trusted team so that suspects are not tipped off. Promptly, an independent assessment should be obtained from litigators of the options, together with how communications should be structured to preserve confidentiality and privilege. An overall strategy needs to be agreed – for example, the nature and scope of the investigations, who will do what and what proceedings may be needed, when and in what jurisdiction. If directors and officers (D&O) insurance is in place, consider when insurers should be notified of a potential claim. Generally, when fraud is uncovered, speed is of the essence and one needs to be agile enough to seek, if necessary, injunctions to recover stolen data, potentially search a target's home or office or freeze their assets before they are dissipated.

Mebane: A company's overall goals and objectives should encompass a position that fraud occurring within its operations is unacceptable, irrespective of the complexity of its business model and supply chain. Any company that becomes aware of allegations of fraud within its business or supply chain should take those concerns seriously and promptly refer them to the appropriate internal resources to initiate a thorough investigation. As instances of fraud continue to become more complex, maintaining a continuous improvement mindset with respect to the appropriate controls and processes in place to prevent fraudulent activity and transactions is key and helps mitigate potential misconduct.

Pasewaldt: In light of the progressively stricter legislation and increasing enforcement activities on both national and international level, companies should take allegations of fraud very seriously and should take proper action to respond to any suspicions. Key elements in this regard are the implementation of formal processes that include relevant reporting lines, clear responsibilities and powers for an internal investigation of the allegations, as well as the proper documentation of such investigations, specifically to prevent financial harm to the concerned company but also to protect its senior managers from allegations of violations of supervisory duties. In the course of a relevant anti-fraud programme, a company can incorporate its overall goals and objectives, for example by stipulating individual requirements in its third-party due diligence process, or refraining from engaging in certain business areas or in relations with third parties from specific regions due to the company's overall business ethics and standards.

O'Shea: It is critical to develop a credible, organised internal plan to investigate and respond to the allegation and use it to develop, if necessary, a strategy with respect to the government, the public and any other key stakeholders. Early decisions about how to handle such an allegation set the tone and can have a significant impact on the outcome – there is no substitute for developing and implementing a credible investigative process from the start. Companies should also bear in mind that their responses to such allegations can speak volumes about how the company's internal controls and culture will be perceived.

Laming: Companies should consider setting up an independent team – an investigation committee composed of people not implicated in the allegations – to conduct an investigation into the allegations. If the allegation relates to their own employee, an internal investigation may be the quickest and easiest way to find out what has happened. If an allegation relates to a third party, for example in their supply team, the company will need to consider whether it is able to investigate the matter itself or whether it is more appropriate to enlist the help of external investigators or the relevant authorities. Firms will need to consider reporting any fraud to the relevant authorities and, in some cases, may be obliged to do so. Firms that believe they have been the victim of a fraud will also want to act urgently to prevent any further acts of fraud being perpetrated on them – for example by suspending implicated employees and closing loopholes in IT systems.

Garrett: All allegations of fraud or misconduct should be investigated by

individuals with experience in doing investigations. All too often, allegations are ignored because they can be dismissed as inaccurate or unfounded, but the underlying activity being alleged is what gives rise to concern. If the person doing the investigation, often a manager, is biased or unfamiliar with how to do a thorough and complete investigation, he or she might miss symptoms of a bigger issue or underlying fraud. Additionally, there should be some level of oversight for fraud-related investigations, such that they are reported up the chain. This provides an early warning system for management to identify fraud, as well as the ability to intervene and drive company values and discipline, if appropriate, given the nature of the allegation.

Goldin: When an allegation of wrongdoing surfaces, it is important to respond quickly and comprehensively. Reports of wrongdoing should be addressed by employees who can fairly, competently and independently evaluate the issues. Depending on the nature of the allegation, it may be appropriate to engage subject matter experts with the experience and the resources to dig in. And careful thought should be given to conducting the review under the direction of counsel to maximise application of privilege and reduce the possibility that the investigative files might later become subject to third-party disclosure. Once the work is complete, companies should consider 'lessons learned' and implement remedial measures to prevent recurrence of any substantiated misconduct.

FW: Based on your experience, what do you believe are the indispensable elements of implementing an anti-fraud system that strengthens, as far possible, internal and external programmes, policies and procedures?

Mebane: Examples of indispensable elements of an anti-fraud system include clear and concise policies and processes, a culture where allegations are encouraged to be raised and those individuals reporting concerns in good faith are protected from retaliation, effective governance and independence when investigating allegations of fraud and other misconduct, senior executive and board of director level support to ensure the correct attention and resources are devoted to the programme, and taking appropriate disciplinary measures when fraudulent activities are identified.

Pasewaldt: The cornerstone of an effective anti-fraud system is a thorough risk assessment that identifies a company's gateways for potential fraudulent activity, based on its business and related specifics. Based on the identified areas of risk, a company should then develop a comprehensive programme that includes a variety of measures to prevent fraud, the minimum requirements for which are the implementation of relevant guidelines and policies, relevant training for employees, a formal reporting process for allegations of fraud, the assignment of responsibilities for internal investigations to verify or disprove such allegations, intervention if the allegations prove to be true, including disciplinary measures if employees of the company are involved, and so on.

Garrett: Creating a culture of integrity is the most critical element of an effective anti-fraud programme. Culture starts at the top and company principles must be articulated and reiterated by management early and often. It is also critical to build a compliance and risk-management programme and team that integrates with the business. 'Paper' compliance programmes and compliance professionals that 'check the box' and do not get out their office and engage with the business cannot effectively manage the litany of risks. To really be effective, compliance and risk must have the autonomy, authority and resources to engage with the business. Ideally, this means that compliance officers 'have a seat at the table' and can access strategic information.

Laming: A thorough risk assessment of the vulnerabilities to fraud, both from within and without, appropriate systemic defences, and the education of employees to recognise and report fraudulent activity, are vital elements to any anti-fraud systems. Conducting risk assessments involves assessing the culture, attitude and awareness among employees about their knowledge of and response to potential fraud or business misconduct. Most firms implement a 'three lines of defence' model, embedding controls in the business, having a compliance function which implements, reviews and monitors the effectiveness of those controls and an independent function such as internal or external auditors providing a final level of review. A genuine desire to prevent fraud, driven by senior management and embedded within the organisation, with strong oversight from the top, is often the most important driver of an effective anti-fraud programme.

Goldin: While an anti-fraud programme needs to be tailored to the specific needs of the company, most well-designed programmes contain certain elements: robust internal controls, policies and procedures that are understandable to employees at all levels, comprehensive employee training, channels for reporting suspected fraud that are widely promoted throughout the enterprise and a strong message from the top that retaliation will not be tolerated.

Colston: I would recommend companies pre-plan, as once a fraud is suspected or uncovered they must act promptly and decide what their objectives are. This requires a cool head to make decisions quickly, based on limited information and without alerting the suspects. Anticipation, training and a strategy planned in advance can mean there is a learned response, thereby minimising mistakes and stress in a difficult situation. It might also reveal gaps in the systems and processes which need to be closed – for example inadequate due diligence is being done when recruiting new staff, or flag that no insurance is in place to cover some of the risks resulting from a fraud, such as investigation and legal costs.

O'Shea: An effective anti-fraud system, like most effective compliance programmes, is one that is part of the corporate culture, from the top down, and that takes a holistic approach to risk management.

This includes designing a system that takes into account regulatory requirements, but does not focus on them to the exclusion of other risks. Another indispensable element is ensuring both a robust compliance and risk management function and a first-line defence by educating and empowering other employees as to how to detect potential fraud, and how to respond when they identify concerns.

FW: How do you envisage the corporate fraud landscape developing in the years ahead? What changes do you anticipate in the way companies mitigate and manage fraud?

Pasewaldt: The corporate fraud landscape will certainly be affected even more by the increasing digitalisation and automated procedures that expose companies to specific risks. Companies are expected to invest more in relevant cyber security programmes to tackle such risks and to reduce vulnerability. Simultaneously, international companies will have to keep up with the stricter legislation and growing demands from regulators globally, accompanied by increasing enforcement activity. In this regard, it will be a challenge to maintain anti-fraud programmes that address the requirements of each relevant jurisdiction, and simultaneously provide uniform standards within a global group organisation.

Garrett: Cyber fraud will continue to be a major issue for companies. In response, they must improve their systems and overall training. This will require compliance and risk professionals to expand their understanding and influence into areas traditionally managed by IT departments and chief information officers (CIO). The roles of the CIO and the chief risk officer (CRO) will likely intersect and their functions will overlap to address these fraud areas, in conjunction with compliance, legal and finance executives. None of the traditional methods of risk mitigation and prevention will be effective to stem the speed with which cyber risks will grow, given the speed of technology, and compliance, risk professionals will need to focus more attention on helping build a true culture of integrity to drastically reduce the risk of internal fraud and mitigate the likelihood that external bad actors will be successful.

Laming: Technological advances in the detection and prevention of fraud and the use of data analytics and AI will continue. AI is now capable of detecting fraud in real-time and being anticipatory rather than just reactive. It is also used to speed up internal investigations, with computer-assisted reviews now processing vast amounts of information, recognising patterns, removing duplicate information and determining relevancy on their own. The nature of frauds affecting the financial world is unlikely to change over the coming years, with consumer fraud, asset misappropriation and cyber crime likely to continue. Firms will likely reach a saturation point in terms of tightening their systems and controls, and ethics and compliance programmes in light of greater regulatory and enforcement scrutiny.

Goldin: Despite the best efforts of many companies, corporate fraud has proven to be an enduring scourge. As the SEC has acknowledged, even the best internal controls cannot prevent all intentional misconduct. As fraud becomes more sophisticated and rogue employees come up with new ways to evade controls, companies will need to refine their programmes and policies to address these new risks, particularly in the cyber space as cyber criminals continue to refine their techniques. At the same time, increased globalisation means more regulators around the world with overlapping jurisdiction. Enforcement efforts by worldwide authorities will continue to exert added pressure on companies to invest in sophisticated surveillance, monitoring and due diligence systems to prevent and detect potential fraud.

Colston: Tech of course, is the Trojan horse for cyber criminals. Any anti-fraud system is dependent on staff buying into the need before they click on a suspicious or an unsolicited email, to flag it with their IT department. Often, IT departments run mock phishing or malware emails to train staff to stop and challenge before they thoughtlessly click on a link which may give an 'in' to the cyber criminals to disrupt and steal confidential data. Such training has to be repeated regularly to keep them informed of how cyber criminals have adapted and changed their attack methods. Going forward, we will likely see more corporates using AI and smart technology to review disparate data quickly in order to identify anomalies and raise red flags for humans to investigate. AI is the only realistic solution when investigating fraud. The Serious Fraud Office's (SFO's) 2018 report refers to the SFO's determined use of AI and intelligent machines to investigate crime. The civil courts have already approved the use of such AI technology to allow parties in a fraud case, to get to the 'hot' documents quickly.

Mebane: It is difficult to predict how corporate fraud will develop in the coming years, but technology and globalisation will continue to affect the landscape within which organisations operate and address potential exposure to fraud. This will require companies to proactively evaluate operating models and organisational procedures to identify control failures and strive to promptly address possible gaps in compliance controls that could unnecessarily or inadvertently expose them to legal and regulatory scrutiny. It also appears that regulators are increasing the focus on individuals, which makes training and fraud prevention awareness for employees particularly important. ■