■ **ROUNDTABLE** November 2019

CORPORATE FRAUD

At a time of geopolitical uncertainty and massive technological advances, corporate fraud is increasing, with cyber crime, particularly in relation to the misuse of data, especially prevalent. There has also been a demonstrable increase in detected bribery, corruption and wider corporate malfeasance. In response, government and enforcement agencies are continuing to ramp up their anti-fraud activities, utilising a range of new legislative tools against companies and individuals. Companies need to track such developments carefully and update their fraud prevention strategies accordingly. ■

THE PANELLISTS

Ravinder Thukral
Partner, Brown Rudnick LLP
T: +44 (0)20 7851 6063
E: rthukral@brownrudnick.com
www.brownrudnick.com

Ravinder Thukral is one of the award-winning 14 litigation and arbitration partners in the London office of Brown Rudnick LLP, which combines cross-border civil fraud, criminal and regulatory expertise under one roof. He has particular experience of banking and finance, civil fraud, shareholder and real estate disputes both in the UK, the Middle East and India. He also advises individuals and companies facing criminal investigation or prosecution by major enforcement bodies. He has experience as a criminal prosecutor and has represented those accused of fraud, bribery and money laundering.

Neil Keenan
Partner, Forensic Risk Alliance (FRA)
T: +1 (202) 849 4688
E: nkeenan@forensicrisk.com
www.forensicrisk.com

Neil Keenan has considerable experience providing accounting and advisory services across a variety of industries and geographies. He specialises in the delivery of forensic accounting services including damages assessment, calculations and testimony, accounting fraud, audit/accounting malpractice litigation, anti-corruption investigations and compliance, and asset misappropriation and embezzlement. Beyond investigations, he brings broad experience that includes claims processing, M&A financial and compliance due diligence, corporate finance, corporate valuations, business recovery and restructurings, and external and internal audit services.

Shamoil Shipchandler
Partner, Jones Day
T: +1 (214) 969 3684
E: sshipchandler@jonesday.com
www.jonesday.com

Shamoil Shipchandler is a former senior officer at the Securities and Exchange Commission (SEC) and the US Attorney's Office for the Eastern District of Texas, where he handled significant high-profile cases and led two offices through tumultuous periods that included government shutdowns, budget reductions and hiring freezes. As a government official he gave more than 180 speeches and presentations about an extensive array of white-collar and cyber security topics.

Sarah Klein
Partner, Kirkland & Ellis International LLP
T: +44 (0)20 7469 2475
E: sarah.klein@kirkland.com
www.kirkland.com

Sarah Klein is a partner in Kirkland's government, regulatory & internal investigations practice group in London, where her practice is focused on the representation of clients in government and internal investigations. She regularly advises on all aspects of UK Bribery Act, financial sanctions and anti-money laundering (AML) compliance. She previously worked as an investigative lawyer at the Serious Fraud Office (SFO), where she focused on the prosecution of complex, cross-border economic crime.

Tapan Debnath
Senior Legal Counsel, Nokia Corporation
T: +44 (0)7342 089 528
E: tapan.debnath@nokia.com
www.nokia.com

Tapan Debnath is a specialist corporate investigation and compliance practitioner. He serves Nokia as head of investigations for EMEA, managing some of the company's most sensitive and high-profile matters. He is also compliance lead for a business group and is acting trade compliance counsel. Prior to Nokia, he spent five years at the UK Serious Fraud Office (SFO) investigating and prosecuting serious cases of bribery & corruption, fraud and money laundering.

James A. Garrett
Leader, Business & Quality Systems, NuVasive, Inc.
T: +1 (858) 320 4554
E: jgarrett@nuvasive.com
www.nuvasive.com

James Garrett serves as a senior vice president at NuVasive, Inc. overseeing the company's regulatory affairs, quality assurance, information technology, cyber security, privacy, compliance, environmental health and safety, and risk management functions. He has served as the company's associate general counsel, as well as the chief risk & compliance officer and global privacy officer. Prior to NuVasive, he worked for DLA Piper LLP (US) where his practice focused on class action and complex business litigation.

Andrew Good
Counsel, Skadden, Arps, Slate, Meagher & Flom LLP
T: +1 (212) 735 3212
E: andrew.good@skadden.com
www.skadden.com

Andrew Good represents corporations and individuals in criminal and civil matters in federal and state courts. He has significant experience representing clients in regulatory investigations, including those brought by the Department of Justice, the Securities and Exchange Commission and the Commodity Futures Trading Commission.

FW: Could you provide an insight into the types of corporate fraud that are typically being seen across the current financial and economic landscape?

Thukral: At a time of geopolitical uncertainty and massive technological development, particular types of corporate fraud are prevalent, such as the rapid evolution of cyber crime, particularly in relation to the misuse of data. We see an increase in reports of bribery, corruption and wider corporate mismanagement involving both the civil and criminal law, with the theft of company assets and business opportunities. Often this is because a corporate has expanded their operations into new and emerging markets, where they have encountered unfamiliar business cultures and practices. Sometimes, their internal systems and controls, which have been developed and refined over many years, have not caught up.

Klein: While the combatting of bribery, money laundering and economic sanctions breaches continues to be a focus, many corporates are now also having to grapple with a range of newer, technology-enabled offences. Cyber and data related frauds have become a necessary priority, and specifically for those corporates which operate in sensitive industries or which process or hold significant amounts of personal data. 'Attacks' of this kind are becoming increasingly common and corporates should ensure that the systems and procedures they have in place are sufficiently robust to counter these risks.

Debnath: Fraud as a species of economic crime knows no sectorial or industry boundaries, though certain forms of fraud are industry-specific – manipulation of benchmark rates is, for example, particular to the financial sector. We have seen a spate of such cases in past years involving Libor, Euribor and foreign exchange rate settings. A common feature of corporate fraud is the involvement of third parties, whether sales or business partners, or another form of intermediary, often acting in collusion with bad actors within the company. There are numerous instances of fraud committed through the creation of slush funds using inflated contract prices or unjustified and excessive discounts which are not passed on to the customer.

Good: Prosecutors and regulators have focused on financial markets and trading-based frauds. Lately, this has centred on manipulative trading practices, and before that there were a string of benchmark-related actions. A second fertile source of enforcement actions has been bribery and kickback schemes. Many of these involve government officials, but commercial bribery is also an area of risk. A third category is where fraudulent acts are used to circumvent sanctions regimes, and such schemes may become more prevalent as those regimes proliferate.

Keenan: Corruption continues to dominate with large-scale settlements announced in an increasing number of international jurisdictions. There is also a growing number of prosecutions involving US sanctions and export control violations, which is perhaps unsurprising given the press scrutiny on international trade. In the US, there remains a stream of accounting fraud cases involving revenue recognition and earnings management. In the UK, attention is directed towards the role the audit profession has played with several large corporate failures. If there is an economic downturn, these cases may increase. Moreover, a slowdown in the economy could result in further employee fraud in the areas of expenses, procurement and conflicts of interest.

Shipchandler: The types of corporate fraud that we are seeing remain largely consistent with what we have seen in past years. These include allegations of US Foreign Corrupt Practices Act (FCPA) violations and other corrupt activities, fraudulent financial reporting, healthcare fraud, insider trading, money laundering, embezzlement and misappropriation of corporate assets. In the US, white-collar prosecutions generally continue to drop as the Department of Justice (DOJ) continues to shift resources to combatting non-white collar cases, such as immigration-related conduct, drug trafficking and violent crime. However, a notable trend is in the increase in coordination between the US authorities and their counterparts in other countries. This should result in more cross-border investigations and prosecutions involving multinationals and their personnel.

Garrett: We continue to see examples of corporate fraud schemes involving technology or device companies alleged to have violated the FCPA or other anti-corruption statutes for, among other things, complex commercial bribery involving the operations of subsidiaries of international companies in foreign jurisdictions.

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?

Klein: The recent money laundering probes at Danske Bank and Swedbank are particularly noteworthy for those operating in the financial sectors and subject to know your customer (KYC) obligations. Not only are the cases notable for their sheer size and scale, but also for the severe reputational consequences they have brought for both the respective financial institutions and wider corporate community caught in their radar. While certain of the investigations are still ongoing, and are likely to continue for the foreseeable future, the cases have already highlighted the importance of having in place not only satisfactory compliance procedures but also effective escalation and accountability processes. As the cases clearly demonstrate, the consequences of not doing so can be grave.

Debnath: Bribery and corruption offences are usually the headline grabbers when it comes to major enforcement cases. Quite often, the acts of corruption that are the subject of the headlines are grounded in some form of fraudulent conduct. In July 2019, Microsoft's Hungary subsidiary was issued with a Securities and Exchange Commission (SEC) cease and desist order and entered into a non-prosecution

agreement with the DOJ, with a total financial penalty of just over $25m. The underlying conduct involved slush funds created through bogus third-party discount schemes, which were intended to be passed onto the end-customer but were instead used to pay bribes to government officials in Hungary and Turkey. Another element of the conduct involved improper travel and gifts to government and non-government customers. At the heart of the schemes were fraudulent misrepresentations by Microsoft employees about why discounts were required, false third-party service agreements and diversion of funds intended for marketing activity. Lessons learned from this case include a reminder of the heightened risk posed by third parties and that they have to be properly screened and monitored, controls that are not regularly tested are prone to failure or being bypassed, and that machine learning (ML) is becoming increasingly sophisticated in proactive transaction monitoring, which is one of the remediation measures Microsoft implemented.

Good: *United States v. Bogucki* is a recent noteworthy case. The allegations were that a trader executed trades to take advantage of his knowledge that a client would be unwinding a large foreign exchange hedge. The trader was indicted on fraud charges. The trader was acquitted after trial but, for corporate entities, the most noteworthy elements of the matter are the implications for the bank that employed the trader. The bank identified the conduct at issue, reported it and showed exemplary cooperation, such that the DOJ declined to require any settlement from the bank. This was the first time that the DOJ used its declination programme in a non-FCPA context. This was a good result for the bank and one that companies in similar situations should be aiming to achieve.

Garrett: Of particular interest are the notable corruption and corporate fraud cases in Brazil, such as those coming out of 'Operation Car Wash', primarily because the cases have a seemingly endless global reach and because they include such complex fraud schemes like Odebrecht's bribery division that was allegedly dedicated to facilitating illegal payments across Latin American and the Caribbean. Numerous countries in South America have been involved and apart from direct participants in the fraud, several other international businesses in Brazil have been directly impacted. Virtually every company with a presence in Brazil has had to strengthen its compliance programme and, in some cases, modify its business practices by exiting distributors, changing partners and so on, to mitigate the risk of doing business in Brazil. In some cases, this has resulted in companies exiting the market or materially changing their business strategy.

Keenan: Although not a sizeable matter, the settlement the SEC reached with an Indianapolis-based freight company in April 2019 has several noteworthy elements. The SEC charged the company of withholding losses of $20m through elaborate buy and sell transactions with third parties. The settlement is indicative of many investigations. First, the company was charged with several elements, including fraud, books and records, and internal control violations. Second, another regulator was involved, with the DOJ also charging the company and seeking the disgorgement of profits generated through such arrangements. Third, significant remediation was required post investigation, with the company required to enhance its internal control environment and cure material weaknesses. Finally, the conduct involved arrangements with third parties.

Shipchandler: In the post-Yates Memo era, there has been an uptick in the DOJ's efforts to hold individuals accountable for corporate fraud. The government's track record on this front has been a mixed bag. Acquittals in significant, high-profile individual prosecutions have exposed some vulnerabilities in the government's theories of individual culpability. Regardless, for companies, the government's continuing emphasis on individual accountability should serve as a reminder of the importance of ensuring, as part of their overall compliance programmes, that corporate directors, officers and employees know and follow applicable laws and rules.

Thukral: Two recent developments are worth examining. First, the Serious Fraud Office's (SFO's) decision not to prosecute a number of individuals following recent corporate investigations and deferred prosecution agreements (DPAs) might give some hope that individual directors are no longer a priority target. This is unlikely and should not encourage companies and senior managers to think that enforcement

> "NO COMPLIANCE PROGRAMME CAN EVER SERVE TO PROVIDE BULLET-PROOF PROTECTION AGAINST SOMETHING GOING WRONG. IF THE WORST DOES HAPPEN, THERE ARE SOME ESSENTIAL FIRST STEPS THAT THE COMPANY MUST TAKE."
>
> TAPAN DEBNATH
> Nokia Corporation

agencies are interested in pursuing the corporate entity to the exclusion of anyone else. Secondly, there are an increasing number of reports of bank fraud being committed as part of a wider campaign of human trafficking. Companies should be aware of recent legislation on human trafficking and its potential impact on the way in which fraud should be investigated and resolved.

FW: If a company finds itself under investigation by the authorities and subject to potential litigation, what general steps should it take in response?

Debnath: No compliance programme can ever serve to provide bullet-proof protection against something going wrong. If the worst does happen, there are some essential first steps that the company must take. First, understand what the authorities are investigating and if the company itself is under investigation, or if it is solely the employees that are under investigation. Second, set up a response taskforce, and determine whether external legal and forensic support is required. If the company is under investigation, it would be prudent to instruct external counsel. Another initial step is to give thought to the overall strategy in terms of legal privilege over any internal investigation, whether it will cooperate as fully as possible with the authorities and handling media interest. Strategy should be kept under regular review.

Good: Getting experienced counsel involved early is critical. There are important initial steps that need to be taken with respect to the preservation of evidence and there can be complicated legal regimes around its collection and preservation. Additional steps are going to depend on the facts and circumstances at issue, and counsel can help work through those.

Keenan: Investigations are often gruelling, time-consuming, expensive and difficult, depending on circumstances. However, some steps must be consistently followed. It is critical that companies collect information and data while observing a host of data laws and regulations, such as data privacy, blocking statutes, state secrecy acts and localisation requirements. Falling foul could result in greater issues, for a company and individuals, than the initial area under investigation. Another essential component is understanding what potential jurisdictions and agencies may have an interest. Enforcement agencies around the world have varying expectations with respect to how investigations are performed.

> ONE OF THE FIRST STEPS TO TAKE WHEN AN INVESTIGATION HAS BEEN LAUNCHED OR LITIGATION IS REASONABLY ANTICIPATED IS TO PRESERVE DOCUMENTS AND OTHER EVIDENCE THAT MAY BE DEEMED RELEVANT TO THE MATTER.
>
> JAMES A. GARRETT
> NuVasive, Inc.

Garrett: One of the first steps to take when an investigation has been launched or litigation is reasonably anticipated is to preserve documents and other evidence that may be deemed relevant to the matter. This would include making a reasonable determination as to likely custodians and witnesses and launching an initial investigation into the factual background. Simultaneously, outside counsel should be engaged and, depending on the nature of the matter, notice of the matter should be disclosed to insurance carriers. Likewise, management and oversight bodies should be made aware of the matter, where applicable. Thereafter, steps should be taken, in conjunction with outside counsel, to develop a thorough and complete understanding of the facts underlying the matter.

Thukral: In so far as possible, it is important to get to grips quickly with the factual and legal basis of the complaint, as this will inform the nature of the response. It is also important to select a separate team of people who are responsible for managing the issues involved. In this way, the corporate response to the complaint cannot properly be criticised for having been implemented by employees or directors who may be implicated in the alleged wrongdoing. A corporate will need an internal and external strategy to deal with questions and requests for information from shareholders, investors, investigators and the press. It may also need to move quickly to secure documents and assets. The early stages of a dispute or investigation are crucial and will likely influence how the investigation or litigation proceeds. In the criminal sphere, a corporate should consider how the SFO's corporate cooperation guidance might apply in relation to issues such as self-reporting and legal professional privilege.

Shipchandler: There are a number of steps a company should take in response to a government investigation. At the outset, it is important to understand that no two government investigations are identical. In other words, each investigation involves its own set of circumstances and therefore deserves its own considered corporate response. In some instances, the response may entail little in the way

of time and effort. In other instances, issues and associated risks may call for a response consisting of a multitude of highly coordinated activities. Particularly for the latter category of matters, it is generally advisable to enlist qualified and experienced counsel to assist with, among other things, appropriate data preservation, fact gathering and legal analysis, as well as engage with relevant government authorities. Where significant legal, financial and reputational risks may be in play, companies often also benefit from public relations and crisis management services. The overall corporate objective is usually to develop, as quickly as possible, a sound understanding of the facts and the legal implications. This, in turn, should enable the responsible corporate personnel to understand, evaluate and act upon the available options for addressing the government's investigation as a matter of sound governance.

Klein: The appropriate response will depend on a range of factors, not least including which authority is conducting the respective investigation and the way in which the corporate was notified of the investigation. Many authorities have set investigation criteria and cooperation expectations set out in published guidance. These should be consulted before any concrete steps are taken. However, as a general matter, common steps taken following the commencement of an investigation typically include the suspension of data destruction processes and issuance of document retention notices, the identification of potentially relevant data repositories, custodians and implementation of data holds across them, the instruction of external legal counsel and developing lines of communication with the investigating authority. Where the corporate was notified of the investigation as a result of the receipt of a document production request, the corporate should, as a preliminary matter, establish with the assistance of external counsel whether the scope of the request can be reduced in any way and what the timetable for production is. Where the investigation commences as part of a search or raid by the authority, the corporate should immediately notify and instruct external counsel and together ensure that the search is carried out in a lawful fashion and within the parameters of the respective warrant or investigative power. Consideration of privilege should also be given at the very outset of any investigation and external counsel should be engaged to assist in ensuring that privilege is maintained from the beginning.

> IT IS IMPORTANT TO SET UP A REGULAR PROCESS THAT WILL IDENTIFY RISKS AND SET UP CONTROLS THAT CAN BE IMPLEMENTED TO MITIGATE THEM.
>
> ANDREW GOOD
> Skadden, Arps, Slate, Meagher & Flom LLP

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?

Good: It is important to set up a regular process that will identify risks and set up controls that can be implemented to mitigate them. The specific risks facing an enterprise will vary based on its business model. There should be clearly identified stakeholders who work on this process and legal and compliance teams should be included. This group should develop a process for vetting third-party relationships that include ensuring that third parties warrant to comply with key laws and regulations and that they have policies governing risk areas.

Keenan: Business partners are key to any business's success, but they come with considerable fraud risk, such as accounting fraud, corruption, export controls and sanctions, and cyber breaches – to name but a few. Companies need to assess third-party risks through a variety of lenses with coordination across departments, such as procurement, legal, compliance and IT. One particularly challenging area is the ongoing monitoring of third parties post contract. Deploying data analytics and dedicated monitoring techniques to assess and respond to changes in the risk profile and business activities are key to helping companies achieve this.

Garrett: The hallmark of any fraud and risk programme is developing effective training and communication. All too often, companies rely on 'one size fits all' training programmes that are easy to disseminate across the organisation, but that fail to increase the skills and training of employees. Many of these programmes, although easy to track via a company's learning management system, are easily discounted or ignored by employees and vendors as a 'tick box' exercise. Compliance and risk officers should develop targeted training programmes and materials tailored

to specific roles and functional areas within the business. Targeted materials tend to be seen as being more valuable to recipients and are more likely to increase awareness and overall knowledge of critical risk areas, thereby increasing early warnings of potential fraud risk. Alongside effective training and communication is the need for management to facilitate open and constructive communication mechanisms, be it through management review meetings, town hall meetings or other governance mechanisms. It is not enough to simply have an integrity hotline or to rely on employees to highlight the issues they identify. Management needs to emphasise the 'tone from the top' and create an environment where issues are raised and vetted without the fear of retaliation. Having an anonymous hotline or reporting mechanism, as well as a formal anti-retaliation policy, is another key component of any good programme. These same processes can and should be highlighted when engaging third parties. Furthermore, contracts with third parties should contain explicit references to the company's fraud and risk policies, including the obligation to comply with said policies, and relevant third parties should be trained on key risk areas, such as anti-bribery and corruption. Likewise, employees who regularly engage with third parties should receive targeted training specific to engaging with risks around third-party engagements. Compliance and risk officers should also conduct routine auditing and monitoring of third-party compliance.

Shipchandler: A robust fraud risk assessment is the foundation for a well-functioning corporate compliance programme. Processes related to third-party relationships merit special attention since these relationships tend to give rise to most fraud and corruption issues. There are good opportunities to mitigate fraud risk at every stage in the lifecycle of a relationship with a third party. In this regard, a company should be thinking critically about its processes for vetting, engaging, onboarding and monitoring third parties, and about paying particular attention to any third parties that may present heightened risk. Specific risk-mitigation measures can include requiring third parties to participate in anti-corruption training and to certify compliance with relevant laws and regulations. To further strengthen controls, companies should consider adding audit right provisions into agreements with third parties and exercising the audit rights to ensure ongoing compliance. It is also important to train those corporate personnel working with third parties on potential red flags in the review of invoices and supporting documentation.

> "WHERE THE INVESTIGATION COMMENCES AS PART OF A SEARCH OR RAID BY THE AUTHORITY, THE CORPORATE SHOULD IMMEDIATELY NOTIFY AND INSTRUCT EXTERNAL COUNSEL."
>
> SARAH KLEIN
> Kirkland & Ellis International LLP

Klein: Key to implementing and maintaining an effective compliance programme capable of identifying potential third-party risk and misconduct is ensuring that the respective programme is tailored to both the overall risks faced by the organisation, as well as those posed specifically by the respective third parties. The starting point will be to carry out a risk assessment which takes account of and assesses both the organisation's respective sector, industry and country of operation as well as the parameters of the proposed third-party engagement. Specific third-party measures that may be introduced following the initial assessment of risk include the inclusion of appropriate financial crime contractual protections, provision for rights of audit over the third party's books and records, mandatory annual compliance certification and mandatory financial crime training as part of the engagement.

Thukral: The approach that a company takes to fraud detection is informed by a thorough assessment of its potential vulnerabilities and the wider business context in which it operates. Once a corporate understands how it may be threatened by fraudulent activity, then it can craft policies, practices and a culture which seeks to reduce its exposure to that threat. Proper planning is a central consideration so that employees and managers know how to act if an incident arises which requires an immediate response. While due diligence on third parties can be complicated and time consuming, it is an essential feature of any fraud prevention strategy. Corporates should also consider their contractual arrangements with third parties on issues around disclosure of information, cooperation and integrity standards.

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 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, acting as the custodians of the company's brand

and reputation. Those third parties may not necessarily see it in that way, however, instead seeking to win the deal at any cost. That is why it is imperative to have a third-party screening and monitoring programme that takes a risk-based approach. Doing so will allow enhanced due diligence to be performed on a needs basis and for conditions to be attached as are appropriate. Conditions could include, for example, compliance clauses in the contract, agreed payment channels, discounts or price changes to be approved by compliance, and monitoring and compliance training to the third party. 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 compliance must be seen and act as a trusted partner to the business, which requires the two to be closely aligned and proactive in its third-party business and compliance strategies.

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

Keenan: Best practice would recommend a company deploy an investigation policy prior to any problem being identified. Such a policy would provide a framework to evaluate and resolve alleged misconduct. Important elements would include communication channels and overall responsibility – often based on who is allegedly involved or knowledgeable of the misconduct – preservation of relevant data and sources of information, and the evaluation of data governance considerations. A means to conduct an early discrete assessment to evaluate the potential legitimacy of an allegation assists companies in framing the issue and identifying the potential scope and expertise necessary to perform the investigation.

Garrett: It goes without saying that all credible suspicions of fraud that are raised should be evaluated and investigated by appropriate personnel. In short, depending on the nature of the claim or allegation, such as those involving senior management for example, independent and outside advisers or counsel should be engaged to avoid potential conflicts of interest or to help ensure that an inquiry is complete and unbiased, and to further support internal recommendations. Documents and other evidence that may logically be deemed relevant to the matter should be preserved and custodians and witnesses should be identified. An initial investigation into the factual background should be conducted in a timely manner and management bodies should be made aware of the matter, where applicable. Thereafter, steps should be taken to develop a corrective action plan designed to address the root cause of the issue. Investigation details, a summary of the findings and the corrective action should be documented, and future work and audit plans should be updated to verify that corrective actions have been effective and that no retaliation has occurred as a result of the claim or investigation.

Klein: When suspicions of fraud arise, there can be a strong temptation to want to reach an outcome as quickly as possible. However, to avoid 'trampling the crime scene' and to ensure that a reliable account is obtained, it is key to develop a thorough investigation plan and to stick to it. While no two investigations will look the same, the investigation plan should broadly detail the location of any relevant data repositories, the steps needed to collect such repositories, the way in which such data will be interrogated, the identity of potential witnesses and the time frames for their respective interview. Consideration should also be given as to how best to ensure integrity of the investigation and, depending on the type of investigation, to maximise legal professional privilege.

Thukral: Once fraud is suspected, it is crucial that robust steps are taken quickly to make sure that information and documents which relate to the incident are preserved and isolated. Without this, companies may not be able to understand fully what has taken place and how to respond. If an internal investigation becomes necessary, it should be conducted impartially and with the support of trusted company management. Once a company feels confident of the results of any investigation, it must then consider carefully how to resolve it. This will likely involve myriad contractual provisions and regulatory requirements and will likely require the input of outside counsel to help make the numerous judgment calls where time and relevant information may be in short supply.

Debnath: If a company finds itself in the unfortunate position of having to respond

> "IT IS THROUGH EFFECTIVE TRAINING THAT EMPLOYEES CAN COME TO FULLY APPRECIATE WHAT IS EXPECTED OF THEIR WORKPLACE CONDUCT AND HOW TO IDENTIFY AND REPORT POTENTIAL MISCONDUCT."
>
> SHAMOIL SHIPCHANDLER
> Jones Day

to an allegation of fraud, it must understand what has happened. This requires the facts to be gathered as fully and as quickly as possible. 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. In such serious cases, the company should involve its external advisers to help it to 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 and the business.

Shipchandler: When suspicions of fraud arise within a company, the first order of business is typically to try to determine, as quickly and cost-effectively as possible, whether fraudulent activity occurred, who was responsible for that activity and what consequences, legal and otherwise, may flow from the activity. It is often just as important, however, for the affected company to analyse the root cause of the matter. How and why did the fraud happen? Was there a controls failure or a lack of a needed control? What additional controls or systems can be implemented to prevent the problem in future? Are employees properly trained on company policy and sufficiently aware of the mechanisms to report potential wrongdoing? Steps taken to remediate the problem and strengthen internal controls are important not just for ongoing operational purposes, but also to help reduce the company's exposure to regulatory sanctions.

Good: Evidence should be preserved. Legal holds should be put in place on relevant data storage and communications systems. Legal and compliance functions should confer and analyse the potential risk exposure from the suspected fraud. If the potential exposure is substantial, outside counsel should be retained to provide advice and coordinate an investigation. Whether or not a determination is made to engage outside counsel, suspicions of fraud should be investigated. Relevant data and materials should be reviewed in a manner that is consistent with law. Interviews of relevant employees should be conducted. If it is determined that misconduct has occurred, it should be remediated, and a determination should be made as to whether it needs to be reported to authorities.

> "BEST PRACTICE WOULD RECOMMEND A COMPANY DEPLOY AN INVESTIGATION POLICY PRIOR TO ANY PROBLEM BEING IDENTIFIED."
>
> NEIL KEENAN
> Forensic Risk Alliance (FRA)

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?

Shipchandler: There is no term more used in the context of corporate fraud than 'tone at the top'. In essence, 'tone at the top' means that a company's leadership embraces, espouses and sets a tone that inspires a culture of compliance throughout the organisation. Tone-setting messages from leadership, however, only go so far. In order to influence conduct throughout the company, such messages should be supported by policies, procedures and systems that operationalise the company's commitment to ethical conduct, such as anonymous reporting systems and a strong anti-retaliation policy. The key to truly bringing a corporate anti-fraud programme to life is usually employee training. It is through effective training that employees can come to fully appreciate what is expected of their workplace conduct and how to identify and report potential misconduct.

Debnath: It is a vitally important element of an effective compliance programme to train staff on their duty to be able to identify misconduct and to respond properly by reporting it to compliance. The key is to give employees the confidence to speak up, even if it is just a niggling doubt rather than a fact-based belief, without fear of being retaliated against or being considered foolish for speaking up on a hunch. 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. Training should ideally be annual face-to-face sessions to as wide a group as possible, in tandem with online training and communications from leaders and line managers. Most large companies are pretty good at this; perhaps it is at the mid to smaller company level that employee

education on this issue is less sophisticated – but of course, the compliance reporting process and training must be proportionate to the compliance risks the company faces.

Thukral: The benefits of staff training on the detection and reporting of fraud can be crucial. Staff form a central part of a company's anti-fraud strategy as they are aware not only of the risks but also how to act once confronted by suspicious activity. When it is provided, training should be engaging, interactive, mandatory and frequent. A workplace culture in which staff know what fraud can look like, such as a phishing fraud, and can communicate their concerns reduces the risk of repeated incidents and penalties. If training is demoted to a single online module or presentation which is delivered and then forgotten about, it is highly unlikely that staff will know when and how to report with confidence.

Good: Employee training is key to fraud prevention. First, it informs employees about what conduct is acceptable and what is not. Second, it can provide employees with information that will allow them to identify and report potentially fraudulent conduct. Third, the existence of a strong training programme is important for establishing the correct 'tone at the top'. It sends a message to employees that the organisation takes misconduct seriously and is willing to expend resources to ensure that it is not occurring.

Klein: Staff play a critical role in preventing, detecting and deterring fraud. Not only are they the eyes and ears of an organisation but their potential actions or omissions can also bring liability to an organisation. It is therefore key that staff are made aware of their respective obligations and are given the appropriate tools to comply with them and recognise behaviours in others that may be contrary to them. While it is becoming increasingly common for organisations to have some form of employee training programme in place, there is significant variation in their respective efficacy. Only those programmes which are tailored to the specific risks an organisation faces and which take account of the differing risks respective employees may face, are likely to be effective in identifying and combatting fraudulent activities.

Garrett: It is important that all managers, regardless where they sit within the organisation, understand and comply with their duties to raise suspicions of fraud and assist with investigations. Training should be targeted and tailored and should provide both examples and context relevance to a particular role. For example, sales individuals who deal with international distributors should ideally receive training relevant to the risks associated with their roles, with specific examples relevant to their role, such as anti-money laundering or anti-bribery. This training would ideally be different from the training given to an employee in a support function, such as human resources which has little to no interactions with third parties, but which should be aware of the importance of ensuring that employees have proper authorisation or access to information. Both sets of employees should receive regular training on reporting suspicious activity and anti-retaliation.

Keenan: It is critical to have employees identify and raise the alarm early when fraud is suspected. A good barometer of a compliance programme is the willingness of employees to speak up quickly when they have concerns of potential wrongdoing. Ideally, this should be through line managers and direct reports, as opposed to whistleblower 'hotlines'. While they have their place, robust programmes not only set the tone at the top but also conduct in the middle. Educating middle management on how to instil the confidence that an employee can speak up without any attribution, blame or repercussions, can identify potential fraud before it becomes more widespread and costly.

FW: How do you envisage the regulatory and legislative landscape unfolding in the coming months and years? Against this backdrop, do you expect companies to enhance their measures to mitigate potential fraud in future?

Garrett: It is good business practice to continue to evaluate, improve and enhance internal processes and training to mitigate potential fraud, regardless of how the regulatory and legislative landscape unfolds. Having said that, companies and risk managers should re-evaluate their risk profile as the regulatory and legislative landscape unfolds and take appropriate steps to reduce risk wherever practicable. Effective risk and compliance programmes

> "THERE IS EVERY REASON TO THINK THAT GOVERNMENT AND ENFORCEMENT AGENCIES WILL CONTINUE TO RAMP UP THEIR ENFORCEMENT ACTIVITIES AGAINST COMPANIES AND INDIVIDUALS."
>
> RAVINDER THUKRAL
> Brown Rudnick LLP

need to be nimble and risk managers should employ self-assessment tools and evaluations to augment or refine annual workplans or long-term workplans to keep up with the evolving risk landscape.

Debnath: We know that the UK, over the past 18 months and longer, has been going through, and continues to go through, a politically turbulent time in relation to the B word that shall not be mentioned. This has meant that other matters such as extending 'failing to prevent' offences to economic crime has fallen down the list of government priorities. However, it is likely that this is a temporary hold-up to the extension of corporate liability to specified economic crime offences, albeit a long one that might go on for some time longer. In any event, any such extension will require companies to carry out an assessment of their compliance programme to understand whether existing controls adequately meet the risks and how they might strengthen or evolve the programme. After all, such reviews are a matter of good practice and a sign of a healthy, mature and dynamic compliance programme.

Thukral: There is every reason to think that government and enforcement agencies will continue to ramp up their enforcement activities against companies and individuals. Not only do they have new legislative tools at their disposal, such as the Criminal Finances Act, but they are also looking to regulate further the way investigations are conducted and coordinated. Use of technology and machine learning tools also means enforcement agencies are likely to get to the 'hot' documents quickly. Companies should track such developments carefully and ensure that they build any such guidance into their fraud strategies where necessary. In the courts, there is also an increasing amount of cross-over between criminal and civil proceedings where allegations of fraud or corruption are being considered. Sometimes, the courts allow both actions to proceed in parallel, which puts great strain on the defendant having to defend on two fronts. D&O policies need to be reviewed carefully at renewal time to ensure they are 'fit for purpose'.

Good: Regulators have been somewhat less active over the past few years. This is likely to change as shifts in leadership in governments or an economic downturn would likely spur regulators to more activity. In the US, the Trump administration has been willing to resolve allegations of misconduct on more favourable terms than its predecessor. In this environment, companies should consider implementing enhanced measures to detect, prevent and report misconduct. It is likely to get more difficult to resolve cases should the political composition of the government or the economic environment shift.

Klein: Proposals, such as the extension of corporate criminal liability to include a general offence of failure to prevent economic crime, show that the trend towards ever greater regulation and the enforcement of breaches against corporates shows no signs of abating. Addressing corporate misconduct and offending remains firmly on the political agenda and it is expected that corporates will seek to ensure that they are prepared. Whether this includes taking only simple steps such as reviewing policies and procedures or larger steps such as the systematic review and assessment of broader economic crime exposure, corporates will need to, and likely will, act. Those corporates which do, will put themselves in the most favourable position should they ever find themselves subject to investigation.

Keenan: While companies are potentially aware of the risk and read about corporate prosecutions, many continue on the basis that such issues "will not happen to us" as "we hire good people and have strong controls". Experience shows that genuine significant attention to fraud risks and compliance programmes happens when industry competitors are subjected to enforcement scrutiny, or even more so, when issues are identified from within. Enforcement trends will continue unabated and will likely continue to increase in international markets as more countries pass legislation around corruption and data privacy, and respond to public outcry surrounding accounting failures and potential fraud.

Shipchandler: The investigation and prosecution of corporate fraud can often be cyclical, with priorities that are affected by, for example, new leadership, public scandals or the allocation of enforcement resources. However, developments in the regulatory and legislative landscape that appear to have a staying power are the increased coordination among US regulatory and law enforcement agencies, as well as between US agencies and their foreign counterparts. There is also an increased willingness by agencies across many jurisdictions to consider the existence of a robust corporate compliance programme as mitigation for allegedly wrongful conduct. Finally, there remains a consistent emphasis on individual accountability across each law enforcement and regulatory agency. In light of updated or new guidance disseminated by multiple enforcement agencies in the US and elsewhere, we would expect to see more companies conducting risk-based reviews of their compliance programmes, as well as continuously testing their implementation and efficacy. Moreover, we also expect to see an increased use of technology as a tool to assist compliance officers to identify red flags. ■