CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2024

VIRTUAL ROUND TABLE

www.corporatelivewire.com

Introduction & Contents

In this roundtable we speak with experts from the Cayman Islands, Hong Kong, India, the Netherlands, and the United States to find out more about the latest fraud & white collar crime trends and regulatory changes. We discuss the challenges of achieving prosecution in complex cases, best practice procedure upon detecting or suspecting fraud, deferred prosecution agreements, and much more.

James Drakeford
Editor In Chief

Meet The Experts

Dominic Wai - ONC Lawyers
T: +852 2810 1212
E: dominic.wai@onc.hk

Before joining the legal profession, Dominic Wai has worked in the banking sector and as well as in the Independent Commission Against Corruption (ICAC).

Dominic's practice focuses on advising clients on matters relating to anti-corruption, white-collar crime, law enforcement, regulatory and compliance matters in Hong Kong, including advice on anti-money laundering. He also handles cases involving corporate litigation, shareholders' disputes and insolvency matters, defamation cases, domestic and international arbitration cases, cybersecurity, data security and privacy law issues, competition law matters, e-discovery and forensic investigation issues as well as property litigation. His clients include Hong Kong listed companies, international companies, liquidators and a broadcasting company.

Dominic is currently a pro-bono legal advisor of a charity that provides a home service for sick children and their families. He is supportive and actively participating in the activities of the charity.

Jenn Schubert - MoloLamken
E: jschubert@mololamken.com

Jenn (Sasso) Schubert is a partner at MoloLamken and an accomplished trial lawyer who represents individuals and companies in criminal and regulatory matters, and high-stakes civil litigation. Jenn was previously a federal prosecutor in the U.S. Attorney's Office for the Eastern District of New York where she was Acting Chief of the Organized Crime and Gangs section. Jenn prosecuted and supervised complex racketeering cases involving money laundering and financial fraud, corruption and obstruction, cross-border issues and terrorism. She also served as law clerk to the Honorable José A. Cabranes of the United States Court of Appeals for the Second Circuit.

Tarun Bhatia - Kroll
E: tarun.bhatia@kroll.com

Tarun Bhatia is a managing director and head of South Asia in the Forensic Investigations and Intelligence practice of Kroll, based in the Mumbai office. Tarun has extensive experience in evaluating, measuring, and monitoring risks across corporate India over the past 15 years and is a well-regarded industry expert for financial services and structured finance.

Tarun advises clients on investments, partnerships, mergers, and acquisitions, and helps them manage their litigation and dispute resolution process by providing investigative services. He has analyzed and evaluated over 1,000 listed and private companies in India, and his diverse client roster includes large conglomerates, banks, financial institutions, and corporations across power, oil and gas, aviation, steel, cement, auto, FMCG, infrastructure, and real estate sectors.

Gerry Zack - Society of Corporate Compliance
E: gerry.zack@corporatecompliance.org

Since 2018, Gerry Zack, CCEP, CFE has served as the CEO of Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA), a professional association devoted to the compliance and ethics profession with 19,000 members across 100 countries. Prior to 2018 Gerry spent more than 30 years providing preventive, detective, and investigative services involving fraud, corruption, and compliance matters and has worked in more than 25 countries. He also served as global chair of the Board of Regents of the Association of Certified Fraud Examiners (ACFE) and for 12 years served on the ACFE faculty.

Meet The Experts

Elisabeth Lees - Claritas Legal
T: +1 (345) 929 0668
E: elisabeth@claritaslegal.com

Elisabeth is Head of Regulatory Law at Claritas Legal and advises clients on a range of financial services regulatory matters including anti-money laundering, counter terrorist and proliferation financing and targeted financial sanctions at the entity and country level. Advice includes remediating breaches and enforcement matters, providing representation from the earliest stages through to court hearings.

Elisabeth has unparalleled experience in the area of financial services regulation, having served as the National Coordinator to the Anti-Money Laundering Steering Group for which she was awarded a Certificate and Badge of Honour for Legal Services in 2022. Her experience in criminal law as a barrister in London and later as Senior Crown Counsel (International Cooperation) in the Cayman Islands enable her to provide expert advice on criminal liability.

Elisabeth holds an LLM in Public International Law (Distinction) and received the University of London Georg Schwarzenberger Prize in International Law.

Elisabeth sits as Deputy Chair of the Health Appeals Tribunal.

David Schreuders - Simmons & Simmons LLP
T: +31 20 722 2301
E: david.schreuders@simmons-simmons.com

David is a specialist in financial and economic criminal law and is a highly experienced defence counsel in corporate crime litigation matters. Apart from being an excellent litigator, he is a strong advocate for the preparedness of companies and advises boards on compliance issues, designs or upgrades corporate compliance programs and conducts internal investigations for proactive remediation.

He has a very broad experience in white collar crime, in a wide range of fraud matters (including complex accounting, banking, securities, environmental and tax), as well as in compliance and regulatory issues for companies, board members or higher level management. He and his team are also experienced in advising on company policies including Environmental, Social & Governance (ESG) due diligence, cybersecurity and cybercrime resilience, anti-corruption, anti-money laundering, safety & health and trade sanctions. David's practice has a strong international focus and is marked by multi-disciplinary aspects of law.

David is a partner in Amsterdam and works closely with other specialists of Simmons & Simmons internationally. He has built up a large international network of specialist peers over the years, which enables him to offer the client an optimum of knowledge and high level experience if there is also an extended scope outside his practice.

David has over 30 years' experience in high profile litigation matters. He has been a partner since 1998 in leading domestic (boutique) and international law firms. David has a long list of publications to his name and is co-author of the Dutch Defence Counsel Handbook (on Tax Fraud) and of the book Financial Law Compliance (on money laundering and crypto currencies). Furthermore, David regularly lectures about Corporate Compliance, Financial Crime and Cybercrime related topics. He is recommended as a leading practitioner in the "Who's Who of Business Crime Lawyers" and is ranked Tier 2 in the Legal 500 and Band 2 in Chambers. David has Master Degrees in Criminal Law and Tax Law. He is a member of the Dutch Association of Criminal Defense Attorneys (NVSA), the International Bar Association (IBA), the American Bar Association (ABA) and a Fellow of the International Academy of Financial Crime Litigators.

Q1. Have there been any recent regulatory changes or interesting developments?

Elisabeth Lees

Lees: In the middle of 2023, an interesting development in the Cayman Islands saw the extension of legislation to ensure that individuals in positions of management or control as well as all regulated entity types would be responsible and could be fined for breaches of the regulatory acts and the anti-money laundering regulations.

Previously, whilst maximum administrative fines for individuals imposed by CIMA were specified, the route by which this could be achieved was not. Additionally, the only entity type specified as being liable was a body corporate, while in fact all types of entities, such as Exempted Limited Partnerships etc., may be licensed to conduct relevant financial business.

Therefore, the amendments make clear that a wide range of entity types may be subject to fines and prosecution for breaches of the acts and regulations and furthermore, that those in positions of management or control (such as directors, partners, or otherwise) may also be held liable.

The Monetary Authority (Amendment) Act 2023:

(i) s42A(2) and s44A enable the Authority to impose administrative fines on and also enable the prosecution of a director, manager, secretary or other similar officer, a partner concerned in the management or control of a partnership, and persons concerned in the management or control of an unincorporated association (where there is consent, connivance or the offence or breach is attributable to neglect).
(ii) s42B prescribes the fines for the entities which are not bodies corporate, which are identical to those for bodies corporate, namely $100,000 for a breach prescribed as serious and $1,000,000,000 for a breach prescribed as very serious.

The other six Amendment Acts namely:

(i) The Companies Management (Amendment) Act
(ii) The Directors Registration and Licensing (Amendment) Act
(iii) The Insurance (Amendment) Act
(iv) The Money Services (Amendment) Act
(v) The Securities Investment Business (Amendment) Act
(vi) The Virtual Asset (Services Providers) (Amendment) Act

a) Amend the principal acts to provide for the liability of partnerships, limited liability partnerships and exempted limited partnerships.
b) Provide for the liability of partners concerned in the management or control of partnerships, and of persons concerned in the management or control of unincorporated associations (where there is consent or connivance or the offence is attributable to neglect).

Tarun Bhatia

Bhatia: India and most other South Asian countries have demonstrated consistent growth over the last 10 years. As the countries move from being seen as emerging markets to developing economies, they have become accustomed to frequent regulatory changes – mostly positive, but some have been challenging and disruptive. Further, with increased flow of capital, we have also seen higher incidence of fraud in the region. In this backdrop, regulators – particularly in India – have increasingly focused on themes of governance, transparency, and accountability. The intent is to support open markets but at the same time protect the interest of investors, especially small investors.

Q1. Have there been any recent regulatory changes or interesting developments?

Tarun Bhatia

The introduction of the Insolvency and Bankruptcy Code in India in 2016 was an important development and has helped release blocked capital. Both the Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI) have become active when it comes to introducing policies and framework to manage and mitigate fraud risks. There is greater emphasis on disclosure, especially by listed companies. More recently, Forensic Accounting and Investigation Standards have been introduced in India to drive standardisation in their investigative approach. However, while trying to address risks, regulators need to ensure that they don't assume that all problems or fraud are alike, and focus on proactively addressing the risk rather than administrative reporting.

There has been increased emphasis on data privacy with both India and Bangladesh establishing guidelines and policies on data privacy and protection in 2023.

Dominic Wai

Wai: The new Virtual Asset Service Provider (VASP) regime that regulates the provision of virtual asset trading platform services in Hong Kong came into effect in June 2023.

Under this framework, anyone looking to conduct regulated virtual asset services in Hong Kong must obtain a license from the Securities and Futures Commission (SFC). To obtain a license, applicants must meet various eligibility criteria including minimum paid-up capital requirements, maintaining professional indemnity or fidelity insurance, having adequate anti-money laundering controls, and ensuring only professional or institutional investors can access certain services. Licensed entities are also subject to ongoing compliance and reporting obligations to the SFC.

The licensing regime aims to balance promoting innovation in virtual asset services while also providing sufficient investor protection and preventing financial crimes.

David Schreuders

Schreuders: In the Netherlands, 2023 was marked by interesting developments in the field of legal privilege issues. The Dutch Public Prosecution Service (OM) decided to dismiss a case against an asset manager after the Civil Chambers in two courts of appeal ruled that the prosecutor had structurally violated the right to privilege. In the fraud investigation into the asset manager, following a raid in 2015, the OM had obtained two million emails, including thousands of emails between the asset manager and their law firm, and had failed to keep them confidential and partly used them in proceedings. The OM openly admitted to having violated the right to confidentiality and making mistakes in the investigation. More should have been done to safeguard the right to privilege.

The OM dismissed the criminal case, but went to the Dutch Supreme Court after it had lost the civil cases which the asset manager's law firm had initiated. The legal issue is uncertain about the way of dealing with privileged information obtained by the OM in the scope of an information order, addressed to a third party (in this case, an IT service provider who failed to filter out privileged emails which ended up in the hands of the prosecutor). The law prescribes that in case of an information order, the filtering out of privileged material must take place under the responsibility of the public prosecutor. The law is not clear as to whether the public prosecutor (or the employees engaged by him) may thereby take cognisance of the content of this information and whether that information may subsequently be used for further investigation. When the law on information orders came into force in 2000, the practice of obtaining millions of emails did not exist yet. The Advocate-General advising the Supreme Court finds that there is a gap in the Dutch legislation. In view of this, he advises the Supreme Court to provide that in future cases, there should be a role for the examining magistrate (rather than the prosecutor) as regards to the filtering out of privileged material when the content of that material will have to be assessed. We are now waiting for the ruling of the Supreme Court on this issue.

Q2. Have there been any noteworthy case studies or examples of new case law precedents?

Jenn Schubert

Schubert: Cryptocurrency litigation no longer appears to be a burgeoning field, as some of the most notable cases this year involved crypto. While previous years have seen prosecutors trying to define the currency tokens and investor suits attempting to keep pace with the ever-changing market, the litigation this year has resulted in significant outcomes, including the prosecution of Sam Bankman-Fried and FTX, as well BKCoin Management LLC, among others. The Southern District of New York (SDNY) charged and tried Bankman-Fried within the course of one year, which is remarkably fast for a white collar case. The United States Attorney for the SDNY has broadcast that this concerted pace was intended to show actors in the white collar space, and within the crypto industry more specifically, that prosecution for serious fraud can be just as expedient as prosecution for more blue collar or violent crime. There was also a record-making settlement reached in the Binance cryptocurrency matter in late 2023. Viewed collectively with other cryptocurrency prosecutions and resolutions, it is clear that the Department of Justice has pursued cases even beyond criminal prosecution, as there have been bankruptcy claims and counterclaims alleging fraud involving Gemini and other major crypto firms. As these suits continue to unfold, precedent in this area will continue to be set and pave the way for future litigation.

Dominic Wai

Wai: As more fraud cases involving cryptocurrency lead to the possibility of taking legal action to claim back that cryptocurrency, one concern is whether or not cryptocurrency is property under Hong Kong law. The case in question was *Re Gatecoin Limited* (In Liquidation) [2023] HKCFI 914. The court's decision brings Hong Kong's jurisprudence in line with other major common law jurisdictions. The ruling is significant because it means that in Hong Kong, cryptocurrencies can be held on trust and are subject to the same legal protections as other forms of property. If a cryptocurrency is involved in a fraud case, it could be recovered as a property like other legally recognised property that could be pursued.

David Schreuders

Schreuders: The ruling of the Dutch Appeals Board for Disciplinary law on Advocates (attorneys at law, external legal counsel) of 2 June 2023 in a case of lawyers acting as independent investigators. The Appeals Board made a distinction between the lawyer as an independent investigator on the one hand (a 'sui generis' category, a role on its own) and the lawyer as investigator in an internal investigation (the classic role as counsellor and defence counsel, governed by Bar Rules and Core Values). It is forbidden for the lawyer or independent investigator to act for clients to which he or his firm is the trusted advisor. Furthermore, this lawyer cannot act in litigation for that client after he acted as an independent investigator for the same matter. The lawyer who conducts an internal investigation as defence counsel for his client in a more classic role, must ensure that he remains partisan and not give up his privilege. The question as to whether a lawyer or independent investigator could make use of his legal privilege and to what extent he could waive it, was not answered by the Appeals Board. They referred the issue to the legislator and to the Dutch Bar as the regulator for advocates.

Q3. Are you noticing any new trends in the types of cases being pursued by regulators or in the way criminals are operating?

Gerry Zack

Zack: The two parts to this question are related. It begins with the manner in which criminals are operating, as fraudsters have gotten more sophisticated in their schemes. While there are still plenty of very basic and easy-to-detect frauds, many have become quite sophisticated and either utilise technology or capitalise on vulnerabilities in technologies. To be clear, I'm not referring to cyber-attacks, but to an increased role that technology plays in connection with internal frauds perpetrated by employees. As organisations deploy new technologies, there are numerous opportunities for tech-savvy fraudsters to discover weaknesses in controls that open the doors to fraud. At the same time, we see regulators modernising their efforts through technology and tech-savvy employees. Nowhere is this more notable than in the significantly increased use of sophisticated data analytics by government regulators and enforcement officials as they identify and investigate frauds.

Another way in which frauds are changing is that it is becoming increasingly common for fraudsters to operate in collusion with one another. The percentage of frauds perpetrated by one individual is declining, while those attributable to multiple perpetrators is rising. This usually makes detection more difficult, since one or more of the critical detective controls that we are relying on is being over-ridden through collusion.

Tarun Bhatia

Bhatia: Yes, as I mentioned earlier, regulators are very vocal about themes of governance, transparency, and accountability. There has been an increasing trend of multiple regulatory investigations on money laundering, anti-competitive practices, securities law violations including front running, among others.

From the government's perspective, there is an emphasis on fighting corruption. In this regard, the Ministry of Corporate Affairs (MCA) in India has also been closely looking at corporate disclosures and working towards identifying shell companies and deregistering them. These initiatives help in creating greater trust in the eco system and reducing money laundering risks.

Increased use of analytics (data and social media) to identify trends and patterns is helping regulators in identifying the perpetrators early.

The rate of cybercrime has increased world over and India is no exception. Within financial services, the regulator is seen fighting this issue on the front foot and working closely with the banks and financial institutions in identifying and reporting these frauds and also catching the perpetrators.

While there is increased vigilance, an area India can improve upon is speedy convictions. It usually takes years to prove fraud and subsequently in most cases the penalty is a minor financial hit. If we want to improve the corporate culture and tackle fraud, there needs to be swift and conclusive investigations and the fraudster should face criminal actions including sentencing and significant financial impact.

"From the government's perspective, there is an emphasis on fighting corruption. In this regard, the Ministry of Corporate Affairs (MCA) in India has also been closely looking at corporate disclosures and working towards identifying shell companies and deregistering them."

- Tarun Bhatia -

Q3. Are you noticing any new trends in the types of cases being pursued by regulators or in the way criminals are operating?

Jenn Schubert

Schubert: In the past year couple of years, the U.S. government has markedly expanded and increased the enforcement of sanctions and export control in key industries, targeting Russia, China and Hamas, among others. In response, there appears to be an uptick in fraudulent action to evade the enforcement of such sanctions. Indeed, in order to continue to profit from sales of fuel, oil, gas, shipping, and technology including artificial intelligence and semi-conductor development, sanctioned actors have engaged third parties to act as middlemen to continue the flow of goods and services. Those middlemen conduct fraud to obtain and pass along exports from sanctioned individuals to clean third parties. For example, a steel producer who previously shipped to a sanctioned Russian entity might now ship steel to a middleman in Turkey. The documentation of the transaction would show that the steel was provided to a Turkish buyer. The Turkish middleman would then reroute the steel to the sanctioned Russian end-user. In short, the uptick in sanctions enforcement has resulted in an increase of fraud.

Dominic Wai

Wai: In Hong Kong, there has been a huge increase in investment related frauds involving cryptocurrencies, e-commerce and penny stock (rump and dump cases). These cases are frequently related to or instigated with the use of social media sites or groups and communities on instant messaging sites.

For cases that relate to listed companies' shares and fluctuation of prices in shares, the Securities and Futures Commission will investigate, but given that sometimes it might also involve fraud and money laundering with syndicated crime elements, the regulator may engage in joint operations with the Hong Kong Police, and such operations have become more frequent.

David Schreuders

Schreuders: In a money laundering context, there is a trend that the Prosecution Service has a special focus on non-regulated sectors and industries pertaining to so-called Trade Based Money Laundering. Investigations have resulted in the finding that numerous legitimate companies are involved in money laundering schemes by foreign criminal organisations. This type of Trade Based Money Laundering is called 'cash integration'.

Dutch companies selling all kinds of small goods with high value –such as technical components, medical devices, liquor or perfumes– are being paid by third parties acting on behalf of the foreign buyers, but the invoiced amounts are broken down into smaller parts with round figures. The third-party payers are unknown to the seller. The paying parties often do not have a presence on the internet, nor an office or place of business. They often disappear after two or three payments, they are active in other industries than the actual buyer of the goods is and the description relating to the banking transaction does not match with the actual trade (e.g. the sale of perfumes but the payment relates to the purchase of a truck). When the seller does not implement and execute an adequate know-your-customer process as regards their buyers and the third-party payers, a risk of culpable money laundering arises.

The abovementioned circumstances of the trade would by all means give rise to asking the appropriate questions pertaining to the source of the payment, in order to prevent allegations that the seller 'reasonably had to suspect' that the money came from a serious crime.

Q4. What unique fraud challenges do emerging markets present compared to mature regions, and what can be done to reduce overall fraud risk across borders?

Tarun Bhatia

Bhatia: We need to keep in mind that fraud is universal. Our global fraud surveys carried out over the last decade show that both developed and emerging markets face high incidence of fraud. However, the reaction time and thus the financial impact is lower in developed markets. Secondly, we have observed that there is limited use of preventive anti-fraud controls and heavy reliance on identification of fraud incidents through reporting. Most companies are in the infancy stage of their fraud controls and monitoring and consequently, suffer higher median loss due to delays in detecting fraud.

However, over the last few years, especially since Covid-19, in my view, there is an increased awareness among companies and its employees about their code of conduct, whistle blowing and fraud reporting. Mitigation of fraud risks can be achieved through consistent development of anti-fraud controls on one hand and strong disciplinary action to create a culture of zero-tolerance. This may look easy in theory but requires commitment and tough decisions from the board and senior management for an effective implementation.

Jenn Schubert

Schubert: Two of the greatest challenges in reducing fraud risk and increasing fraud prosecution abroad are: (i) corruption within foreign governments and justice systems, and (ii) still-developing regulatory frameworks with little precedent for guidance.

First, corruption in the very justice system that is intended to enforce anti-fraud measures creates a significant stumbling block. Corruption among foreign government officials and governmental bodies must itself not be tolerated. Beyond continued changes of power through election, there are also prosecutorial hooks within the United States to assist in ousting corruption, including FCPA-related prosecutions. One way in which private sector attorneys can assist in the prosecutorial enforcement effort is by representing and aiding whistleblowers abroad who may be able to assist in bringing forth complaints against foreign officials. The U.S. has strong whistleblower protections and can often provide the support needed to bring anti-corruption actions.

Secondly, while new regulations and laws are being introduced in foreign countries aimed at reducing fraud, the laws are relatively untrod. This results in ignorance of their existence or "loophole" defences against them. The passage of time and continued use of these laws will in part ameliorate this issue. In the interim, it is possible for more attorneys practicing in developed systems of justice to offer guidance and comparative lessons to clients and companies abroad. For example, while securities regulations may be new in certain countries, the United States may point to its comparable regulations and impart lessons learnt about how these can be effectively enforced and what compliance efforts overseas companies and clients can take. In other words, ensuring a contoured understanding of the rules will ultimately support their enforceability.

"Corruption among foreign government officials and governmental bodies must itself not be tolerated. Beyond continued changes of power through election, there are also prosecutorial hooks within the United States to assist in ousting corruption"

- Jenn Schubert -

Q4. What unique fraud challenges do emerging markets present compared to mature regions, and what can be done to reduce overall fraud risk across borders?

David Schreuders

Schreuders: In the Trade Based Money Laundering and cash integration context as described in response to the previous question, underground banking with respect to emerging markets is a means of funnelling illicit funds to parties which are able to use front companies to bring the criminal cash into the banking system ('placement' in terms of money laundering schemes). A robust know-your-customer or client due diligence system in mature regions is a way to reduce the money laundering risk. However, the problem is that contrary to regulated sectors under the AML legislation (banks, financial market participants, lawyers, notaries, auditors, traders in jewellery and art, casinos, etc.) which are aware of their sector risks and are heavily regulated, industries and sectors which do not fall under the AML regime often do not have the know-how, processes and sophistication to help them assess money laundering risk and exposure to liability attached to it. In fact, the Prosecution Service is their regulator, but when the prosecutor has come into play, a situation of criminal enforcement has then already arisen.

In terms of anti-corruption, strong and clear enforcement policies in mature markets regarding corrupt practices of their companies in emerging markets, is key. A level playing field should be created and impediments for cross-border prosecution and criminal investigation, for example, too strict jurisdiction rules should be moved out of the way (which the EU already has done some five years ago).

Q5. What steps do you believe governments and regulatory agencies should take to improve fraud protection and strengthen compliance?

Elisabeth Lees

Lees: Governments and regulatory agencies should ensure that guidance is available to assist regulated and non-regulated entities with the prevention of fraud. Typologies and red flags should also be included as well as any recent trends or new developments of which entities should be aware. Regulatory agencies should offer outreach sessions to assist in raising awareness and also to facilitate constructive engagement with private entities.

International cooperation should be utilised by governments and regulatory agencies to its fullest extent. The Egmont Group is an excellent method for Financial Intelligence Units to exchange information, make requests for further information, and to spontaneously disclose information which may be of relevance to another jurisdiction. Regulators should also engage in informal international cooperation, particularly where this information may assist law enforcement in identifying and detecting criminality. Law enforcement to law enforcement exchanges are extremely swift and can be the most effective method to ensure immediate notification between officers in relation to international matters as well as the use of Interpol. Mutual Legal Assistance requests take longer but are required once evidence is needed for court proceedings.

Information from such agencies on the number and types of requests received and any relevant typologies can in turn assist industries in relation to where their own efforts should be focused.

Ensuring that breaches of requirements – such as failing to report suspicious activity or failing to conduct customer due diligence – are properly investigated and, in appropriate cases, enforcement action is taken by the police or the regulator assists in increasing compliance is important as it acts as a deterrent to others.

Q5. What steps do you believe governments and regulatory agencies should take to improve fraud protection and strengthen compliance?

Gerry Zack

Zack: Two things come to mind. First, more governments should establish programmes that reward companies for establishing well-designed compliance programmes. No programme is perfect, and most governments and regulatory agencies recognise that. Frauds and compliance failures can occur even in well-designed systems of internal controls. But when they occur, the degree of any penalty imposed should vary based in part on the efforts taken to prevent the failure from occurring. Reduction in penalties should be a benefit for organisations that take reasonable preventive efforts by designing and implementing sound controls. Likewise, penalties should be increased for organisations that fail to take reasonable efforts to guard against the failure.

The other thing that governments can do is to provide sufficient guidance regarding the nature of controls that organisations should be expected to have in order to earn the reductions in penalties I just described. Creating expectations, sometimes in the form of lofty but vague goals, without corresponding guidance is a recipe for problems. Sound and sufficiently detailed government guidance is crucial to the improvement of fraud protection and compliance.

Dominic Wai

Wai: One important move is establishing a centralised fraud reporting system that collects reports from both public and private sectors. This database can help identify patterns and organise timely, coordinated responses across multiple organisations.

Q6. To what extent does the complexity and sophistication of corporate fraud and white collar crime pose to the legal sector in its efforts to successfully achieve prosecution?

Elisabeth Lees

Lees: The large volume of material required in relation to cross-border white collar crime means that there is a lengthy, resource intensive disclosure review requirement. This can pose a challenge, particularly for smaller jurisdictions.

Furthermore, where predicate crimes for money laundering have been committed in other jurisdictions, this will often require international legal assistance requests to be sent and responded to in order to secure evidence to produce at court. This can be a lengthy process and can lead to delays whilst the prosecutor awaits the response of the Requested State. Best practice dictates that investigators begin with informal cooperation whereby there is law enforcement to law enforcement international cooperation as well as the use of the Egmont network to make enquiries and secure information. Whilst this information cannot be used in evidence, it is useful in ensuring that formal international cooperation requests are targeted and specific and also ensuring that the requested evidence is within the possession of the person from who it is requested. Furthermore, personal contact and the use of networks such as Arin Carib in the Caribbean, the informal asset recovery network, means that the process can be swifter as there is contact with a named individual with whom follow ups can be made.

Q6. To what extent does the complexity and sophistication of corporate fraud and white collar crime pose to the legal sector in its efforts to successfully achieve prosecution?

Gerry Zack

Zack: Explaining sophisticated frauds in a concise and clear manner to individuals who may not have a very good understanding of the technical aspects underlying the fraud is very challenging. I've seen some talented investigators who conducted very complex investigations fail during this stage of the process. Communicating complicated frauds in a manner that makes it clear what happened and how the perpetrator(s) carried out the fraud requires a very different set of skills than those used in performing the investigation.

Simple fraud schemes are easy to explain. Complex schemes involve several factors that make explanations difficult, including large volumes of data and documentation, multiple subjects and witnesses needed to communicate what happened, complex and overlapping timelines needed to illustrate relationships, and many others. Add in the need to explain how technology played a role in the scheme and it makes for a difficult task. It can be easy to confuse listeners or come across as creating false connections if the timeline, methods, relationships and relevant facts are not communicated properly.

Jenn Schubert

Schubert: Certainly, investigations into corporate wrongdoing can be quite complicated as a matter of both fact and law. Often, white collar schemes target the forefront of market opportunity, testing the limits and bounds of the law with the hope that such risk-taking behaviour will ultimately lead to a benefit. Cryptocurrency is a good example of this phenomenon, where it was relatively unregulated upon its inception and so market actors were able to move quickly in attempts to profit from trading without the strong walls of securities regulation. In time, of course, and following litigation, increased regulation and enhanced investigative techniques, the law caught up to the behaviour and crypto is no longer the market forefront of unregulated opportunity.

Secondly, white collar schemes are typically intelligent and executed with savvy. They may thus evade typical methods of criminal investigation such as surveillance, reviewing SARs, or executive search warrants. Unlike an investigation into a drug dealer, with white collar crime there are not hand-to-hand transactions to be monitored, there may be no physical evidence to be seized (like drugs, firearms or the like), and communications may be off-channel or in person. In many instances, successful prosecution may require an insider to cooperate with the government explaining the scheme, offering access to private files and correspondence and recording in-person conversations with conspirators. Getting a "hook" into an insider is often also more complicated as white collar parties less frequently have a criminal record or other entry point, in contrast to, for example, a drug dealer with information about a murder who may be arrested in possession of drugs giving investigators leverage. Typically, the government must independently investigate each individual potentially tied to the white collar scheme to detect and establish their involvement in unrelated activities such as tax evasion, in the hopes of finding a point of leverage that might lead to cooperation.

Even after identifying applicable criminal statutes and developing evidence through a long-term, creative investigation, white collar prosecution may still be challenging as such defendants often have the means to litigate the cases thoroughly, offer mitigation to evade custodial sentences, and provide complex expert analysis remediating culpability or financial liability.

Q7. How important is collaboration between different regulatory agencies, law enforcement and private sector entities to improving fraud protection?

Elisabeth Lees

Lees: It is extremely important that there is close collaboration between different regulatory agencies and law enforcement. Complex fraud and money laundering schemes will often involve regulated entities such as banks or trust and corporate service providers, and even if they are not the perpetrators, evidence will be required. The regulator may also consider an investigation into whether sufficient preventative measures were in place. The regulator may have additional information the police were unaware of. Additionally, regulators can reach out using direct lines of communication they have established with their overseas counterparts, for example, where there is supervision of a group. This can enable further information to be shared swiftly. The police need to be aware of potential regulatory breaches in order to share relevant information with the regulator in order for the regulator to investigate those breaches.

Collaboration between regulatory agencies, law enforcement and the private sector is essential to ensure that the private sector is updated in relation to the latest cases and trends. The private sector should also share their own typologies and encounters with the police and regulators in appropriate forums (sanitised). The private sector also needs to be aware of the circumstances in which they need to make contact with their regulator or the police. Furthermore, the private sector should be made aware of the criminal penalties and the regulatory penalties which are applicable for matters such as failing to report suspicious activity as this may assist in increasing awareness and compliance.

In the Cayman Islands, the Supervisors' Forum was established to ensure that the regulators could meet regularly and discuss trends, any legislative changes required, issues encountered, and potential solutions. This ensures that the four supervisorsmeet regularly and exchange information.

The Stakeholders' Forum was established to enable regular interaction between law enforcement and industry. The Cayman Islands Bureau of Financial Investigations (the unit of the Royal Cayman Islands Police Service responsible for complex money laundering and terrorist financing investigations) meets with industry members across sectors such as banking, trust and corporate service providers and others. Presentations are given on relevant topics by both industry representatives as well as public sector representatives such as the Financial Reporting Authority. The sharing of sanitised typologies and recent trends and developments is encouraged. Public-private partnerships are widely recognised as an extremely effective and essential tool to combat complex money laundering – utilising the knowledge, skill and IT resources of industry.

Tarun Bhatia

Bhatia: Often, one fraud incident is perceived as a violation under various statutes and hence various regulatory bodies, law enforcement agencies and government departments are involved in the investigation. In our experience, regulatory matters are long-drawn, sensitive, and often subject to high media attention. Therefore, a collaborative approach between various regulatory and law enforcement agencies is the most ideal. However, this is easier said than done.

Often, regulatory bodies and government agencies operate independently without seeking inputs or understanding the implications. The most common examples are changes in tax laws which have far reaching impact and often genesis of incremental fraud. Furthermore, often in investigations, different authorities approach the matter differently leading to a long process with limited successes. Similarly for private sector to cooperate, there needs to be greater transparency and information sharing by regulatory agencies and law enforcement. This will create trust and will lead to better outcomes and improve fraud protection.

Q7. How important is collaboration between different regulatory agencies, law enforcement and private sector entities to improving fraud protection?

Jenn Schubert

Schubert: Collaboration is essential to successful fraud protection. Regulatory agencies, law enforcement and private sector entities each have unique access and tools to gather and analyse the information needed to detect and prevent fraud. For example, law enforcement may execute search warrants or rely on wiretaps or other surveillance while private sector entities have internal access to KYC data and historical sales patterns versus aberrations. Pooling such sources of information together creates a complete picture, revealing the full scope of a fraudulent scheme. It is then incumbent on regulatory agencies to take enforcement action partly to put an end to ongoing fraud and also to deter similar schemes. If all actors and entities make clear that fraud is being monitored and will not be tolerated, and offer clear guidance and enforcement mechanisms, there is a generally stronger probability of anti-fraud compliance.

Dominic Wai

Wai: Collaboration across regulatory agencies, law enforcement and private sector entities is incredibly important for enhancing fraud protections in Hong Kong. As fraud tends to use new technologies and social media, coupled with cross border or boundaries threats, their combined powers and resources would be needed to tackle high stakes and mass victim cases.

By collaborating, the regulators and law enforcers can share information and intelligence. It would allow better recognition of trends, patterns, and emerging fraud modus operandi, and enhance their ability to move quickly to tackle the new cases and risks.

With collaboration, limited security resources across organisations achieve more through concerted efforts against shared objectives. Hence there had been more collaboration between regulators and law enforcements with more memorandums of understanding being signed between regulators and law enforcement agencies to synchronise joint operations such as dawn raids.

David Schreuders

Schreuders: Public-private collaboration is key because there are clear benefits for both sides. The private sector could rely on international treaties for mutual legal assistance in criminal matters and cross-border investigation powers from the public sector (the Prosecution Service). Similarly, the public sector could rely on the results of corporate investigations into the facts. There are advantages in terms of speed and the effectiveness of combatting (international) fraud. Dutch prosecutors often raise the option of public-private collaboration when I discuss with them fraud schemes which have victimised my clients and the possibility to press charges against the fraudsters.

Q8. How can companies best respond to detected or suspected cases of fraud in a measured and consistent manner? What response tools help restrict and minimise losses?

Elisabeth Lees

Lees: Regulated entities are required to have policies and procedures to assist in preventing and detecting primarily money laundering (alongside terrorist financing, proliferation financing and sanctions evasion) but these also assist in the detection of white collar crime generally. These include customer due diligence checks where adverse media reports, such as investigations overseas, should be detected, systems to identify politically exposed persons who may be susceptible to corruption, and robust sanctions' screening procedures to identify not only if the person themselves is designated but whether they are acting on behalf of a designated person. More broadly, ensuring that entities know the nature and purpose of the business of their client and the reason for the relationship allows them to establish whether there is a legitimate purpose for transactions or any reason for suspicion.

Understanding complex structures and who the beneficial owners are assists in identifying any links between those who own and control a structure and the transactions or any linked structures, which increases transparency and the ability to detect if there is a fraudulent scheme between entities which cannot be detected by looking at the entities alone. Carousel frauds often involve numerous entities in different jurisdictions and layering behind the front companies means detection is only possible where those in control of the entities are identified.

It is best practice for other entities who are not regulated to replicate procedures and policies in some of these areas to assist in their own fraud prevention and detection initiatives, even where these are not mandated.

Another important area is that of reporting suspicion. Front line staff should be trained on typologies and red flags and the procedures for reporting. For regulated entities, a designated money laundering reporting officer receives these reports and decides whether a suspicious activity report should be filed with the Financial Reporting Authority ('the FRA', the Financial Intelligence Unit for the Cayman Islands). The FRA then analyses the report and other information to determine whether a dissemination should be made to the police for further investigation.

Whilst the Cayman Islands does not currently have a 'consent' regime, whereby a request for consent to move funds must be authorised before continuation, legislative changes made in October 2023, will enable the establishment of such a regime when enacted in the near future. Currently, the FRA has the power to freeze funds for up to 30 days to enable investigation and consideration of a formal restraint application by the police.

A designated person who is responsible for conducting internal investigations and liaising with the police and regulators is essential for regulated and non-regulated entities to ensure there is a central point for any internal investigation and clear and consistent engagement and exchanges with law enforcement. Reputational damage must also be considered and catered for, to the extent this is possible without compromising any ongoing investigation.

Gerry Zack

Zack: It begins with establishing the earliest methods of detection possible. Frauds will happen in even the most well-designed systems of controls. The key to loss minimisation is early detection, whether in the form of reporters bringing it to our attention through a well-publicised and easy to use reporting system or through other detection methods. This is where proper use of data analytics plays an important role. In today's environment, most activities involving fraud leave a digital trail throughout parts or all of a fraud. This digital evidence may reside in accounting and financial systems, security systems, shipping and receiving data, or in any of a wide variety of data sources and systems.

Q8. How can companies best respond to detected or suspected cases of fraud in a measured and consistent manner? What response tools help restrict and minimise losses?

Gerry Zack

Once an organisation takes a proper inventory of the data it has, a process analysis can be done to determine the flow of data, the controls at each step of the process, and who is involved in accessing, updating, or changing the data. Once this is done, it becomes possible to profile what characteristics in the data would differ in a fraudulent transaction or activity in comparison with a valid one. That's the key to establishing an effective and efficient data analytics programme that can detect frauds in their earliest stages. These same data analytics techniques that may be used to detect frauds can also be used to assess allegations of fraud.

One additional point that is important here involves the most common criticism of data analytics – that it can produce numerous "false positives", instances in which transactions are flagged as being suspicious, only to be determined to be legitimate upon further inspection. The key to minimising false positives is in the design stage. Careful consideration of what would distinguish fraudulent from legitimate activities takes time and requires a solid understanding of how data is impacted (i.e. what should be expected of digital evidence) by fraud. Often, basing conclusions on a single digital factor produces more false positives than utilising tests that assess multiple characteristics.

Tarun Bhatia

Bhatia: Respond judiciously and take informed decisions. Hurried responses often lead to incomplete and incorrect conclusions and reporting. First and foremost, it is important for companies to implement an easy and trusting whistleblowing mechanism. I have seen cases where companies have a whistleblowing process but it's not employee friendly. Often these are only in one language (English) while employees could be spread across multiple cities and countries. The other mistake many make is only having one option (voice or email) but not everyone is comfortable in one mode. Lastly, the contact point is often the business head and not an independent team or person. Because of these issues, many incidents don't get reported. Also, as a best practice, companies should have a fraud risk or incident response team and all the information flow related to any investigation should be pivoted through this team. This will help in keeping the investigation focused and avoid unnecessary water cooler talks across the organisation.

Fraud often leads to substantial financial loss and there are ways to mitigate that too. In one of the matters that we recently assisted with, our client triggered its fraud insurance claim immediately upon reporting the matter to the board and engaging an independent firm for investigation. A Steering Committee constituting independent directors, nominee directors and general counsel was formed to identify, detect and quantify the impact of fraud. This assisted in delineating the process of fraud assessment and quantification from the ongoing business operations. Similar to this, companies can adopt other procedural or tactical means to restrict and minimise losses.

Dominic Wai

Wai: Companies should have standardised policies and protocols to ensure speedy responses and consistency in handling each case. A core fraud response team should be set up, comprising representatives from management, technical teams (e.g. IT teams) and the legal department (for legal advice and preserving legal professional privilege) to direct the process. Outside counsel and professional investigators and consultants (e.g. forensic accountants) might also need to be engaged.

This team's first task is confirming the type and scope of fraudulent activity using tools like forensic accounting software. If the matter concerns ongoing leakage of data, response technologies such as IP blocking, login access revocation and restricted fund transfers can help contain potential losses by quarantining the threat. Civil legal action to freeze suspect accounts and transactions may prevent ongoing danger while under review.

Q8. How can companies best respond to detected or suspected cases of fraud in a measured and consistent manner? What response tools help restrict and minimise losses?

Dominic Wai

After seeking legal advice, companies might want to notify law enforcement for investigation and pursuing the culprits, which might come up with information and evidence to help with the civil legal action pursuit. If there is insurance coverage for the fraud case, the insurance company would need to be notified. Meanwhile, it is important to reassure legitimate customers and partners through internal and external communications.

Auditing practices post-incident can strengthen the weak points revealed.

David Schreuders

Schreuders: A corporate investigation into the facts is commonly the most effective tool to minimise losses and to mitigate legal liability risks. Based on the findings of the investigation, I will be able to advise my client how to act. Disciplinary measures could be necessary or appropriate, civil cause of action could be applied to the fraudsters in the context of asset recovery, or self-reporting to the regulator or the Public Prosecutor would be a good way to minimise fines and mitigate other negative risks for the company.

Finally, an internal compliance assessment is an adequate tool to measure the level of compliance within the company, which could be helpful to adjust the corporate compliance system if the outcome of the assessment would point in that direction.

Since June 2023, Dutch lawyers have to be very clear about their role as an investigator. A corporate investigation into the facts conducted by the lawyer in order to advise his client on the way forward in a litigation context, and while preserving his legal privilege, is the classic role of a lawyer in a Dutch legal context.

Q9. Under which circumstances is a deferred prosecution agreement recommended, and how are they utilised in your jurisdiction?

Elisabeth Lees

Lees: Deferred prosecution agreements are not available in the Cayman Islands. There is no formal plea-bargaining system. If a plea is entered to one of a number of charges, the prosecution will consider whether it is in the public interest to continue with any of the remaining charges. This will include consideration of the likely penalty, and whether the level of criminality is sufficiently captured in the charge to which the guilty plea pertains, amongst other matters.

Deferred prosecution agreements have been recognised as an alternative to conventional prosecution because of lower risks and costs for the prosecution in other jurisdictions, with the advantage of still incorporating an admission of corporate wrongdoing and a requirement to remediate, as well as a substantial penalty. As corporate and financial crime is increasingly complex and resource intensive, deferred prosecution agreements can offer an alternative to lengthy and costly proceedings, if used appropriately.

The Cayman Islands legislation provides for the prosecution of natural and legal persons as well as for vicarious liability for particular white collar crimes as identified in the legislation.

Q9. Under which circumstances is a deferred prosecution agreement recommended, and how are they utilised in your jurisdiction?

Elisabeth Lees

The Bailiwick of Jersey, a Crown dependency has introduced deferred prosecution agreements.[1] The Cayman Islands, an overseas territory follows a similar two-stage test in determining whether to lay charges in a matter namely: (i) the sufficiency of the evidence and (ii) the public interest. Under the Criminal Justice (Deferred Prosecution Agreements) (Jersey) Law 2023 ('the DPA Law'), the question of whether a DPA is in the interests of justice is considered in cases where a self-report has been made and factors such as the degree of harm and previous enforcement action taken are considered. The question is then whether it is appropriate to enter a DPA, notwithstanding the public interest of prosecuting. It will be interesting to follow the development of this regime and review whether the Cayman Islands considers it appropriate to introduce a similar provision.

1. Deferred prosecution agreements in Jersey: Ways to buttress the castle. A comparative analysis of regimes for deferred prosecution agreements in Jersey and England and Wales. Bastian Herstein, Matthew Berry and Sam Brown, Journal of Economic Criminology, September 2024.

Jenn Schubert

Schubert: In the United States, a deferred prosecution agreement may be extended to an individual or a company. It is most frequently offered when: (i) the target is cooperative, (ii) there is immediate effort made to correct the wrongdoing and strengthen future compliance, and (iii) there are other applicable mitigating factors.

First, a target seeking a deferred prosecution is typically cooperative with the government's investigation. That cooperation does not have to be (and often is not) formal pursuant to a cooperative agreement. Rather, 'cooperation' is typically informal wherein the company or individual responds promptly to requests for documents or proffers, is fulsome in its disclosures, and freely offers information regarding its own conduct and that of other potential wrongdoers. Cooperation may span the course of a government investigation, from early subpoena requests all the way through to the indictment of other targets. This may in effect require years of patience and responsiveness, which also provides the target with ample opportunity to improve its own standing.

Second, and perhaps one of the most significant ways in which a target may improve its standing with the investigative agency, recipients of deferred prosecution agreements are typically dedicated to remediating potential wrongdoing and improving their compliance. This may initially involve an internal investigation or review of the conduct or individuals the government is investigating. A target may retain independent counsel to conduct such an inquiry. Upon identifying problematic areas or potential ways to improve compliance, companies and affected individuals seeking deferred prosecution would typically take such measures by, for instance, restructuring, revising compliance systems, enhancing reporting requirements, or otherwise substantiating insufficient processes. The improvements should be meaningful and long-term.

Finally, in the United States, deferred prosecution is most frequently considered as a resolution when mitigating factors are present such as relatively lesser culpability or lack of knowledge; a weakness in admissible evidence or proof of key elements to establish wrongdoing; indicia of actual innocence, duress or other affirmative defences. The onus is often on the target to proffer mitigating factors to the government for its consideration. Attorneys for the targets may provide mitigating evidence showing a lack of knowledge, a true defence, or, often, contextual evidence regarding why the company or individual acted as it did – perhaps a good faith belief it was acting lawfully, extenuating circumstances such as personal challenges, and so forth. Mitigation packages may be presented in writing, orally, or some combination thereof.

Q9. Under which circumstances is a deferred prosecution agreement recommended, and how are they utilised in your jurisdiction?

Jenn Schubert

It is important to understand that in the United States, a deferred prosecution agreement itself typically outlines strict terms that the target must abide by, including remediation steps or compliance directives, strictures on the individual or company's ability to participate fully in the market, restrictions on the individual's personal life or movement, and other stringent requirements the violation of which could result in termination of the deferred prosecution agreement. Should the target fail to comply with these terms resulting in loss of the agreement, the government has a preserved right to initiate a prosecution notwithstanding the passage of time.

David Schreuders

Schreuders: A deferred prosecution agreement ('settlement') is quite common in the Netherlands and is in principle applied to corporates, not individuals. The process is being governed by Guidelines from the Advocate-Generals' Board, the highest body within the Public Prosecution Service, above certain thresholds (a fine of €200,000 or more, or a total value of €1 million or more of the settlement when disgorgement is applied or damages should be compensated). The Chief Prosecutor, the independent Settlement Commission and the Advocate Generals' Board will have to give their consent. Furthermore, an element of transparency is added, as a press release from the Prosecution Service is mandatory as well as publishing a Statement of Facts on the Prosecution's website.

The Public Prosecution Service prefers deferred prosecution agreements rather than bringing the case against the corporate to court, because in the latter situation it will not be possible for the judge to impose all kinds of compliance improvement measures. The prosecutor will be able to do so in the context of stipulating those measures in the settlement agreement with the corporate.

It is important to realise that the corporate will only have to admit facts, but not guilt, culpability or legal qualifications of crimes (allegedly) committed.

Q10. How can education and training be utilised to equip professionals with the knowledge and skills necessary to combat emerging threats?

Elisabeth Lees

Lees: Professionals are engaged in their own industries and have their own competing demands as well as ensuring that their clients' needs are met and targets are reached. Without the necessary education and training in emerging threats, which should be conducted on an ongoing basis, they cannot be expected to detect complex fraud or money laundering schemes which are set up in a manner to avoid detection. In fact, the Cayman Islands' legislation provides a defence for failing to file a suspicious activity report, where the employee has not been provided sufficient training by the employer.

Education and training on typologies is one of the most effective means of raising awareness of professionals to schemes which may affect their own businesses. These should be accompanied by red flags which professionals can then make a note of in case they are encountered. Areas of higher risk, such as virtual assets, should also be covered. It is also useful to train professionals on the country's national risk assessment so that they can be aware of threats at a national and international level as well as at the sectorial level, for which reference should also be made to risk assessments conducted by regulators in the country. Risk assessments should not just be reviewed for the sector in which the professional operates but for the sectors in which the professional's clients operate. For those conducting international business, training should include those countries of particular concern to their line of business. This may include identifying countries of higher risk for money laundering (e.g. by looking at the Financial Action

Q10. How can education and training be utilised to equip professionals with the knowledge and skills necessary to combat emerging threats?

Elisabeth Lees

Task Force lists) or those at higher risk for corruption (e.g. by looking at Transparency International's Corruption Perceptions Index). Where a professional works in an industry of higher risk or has customers in such an industry, this should also be identified and the red flags and typologies reviewed.

Once the risks have been identified, the policies and controls in place to assist in detecting and preventing such threats should also be explained and training provided. The training should reiterate the reason for the measures as well as the consequences of non-compliance. Professionals are far more likely to follow policies and procedures when they understand the reasoning for them. Additionally, as above, with many competing demands it is important that they are reminded of the importance of compliance.

Gerry Zack

Zack: Continuing education and training are absolutely essential to managing fraud and compliance risks in today's environment. Fraud schemes and compliance risks are evolving at a faster pace than ever, often driven by the equally fast pace of the development of new technologies that can be used for good or fraudulent purposes. Keeping up with the tools and techniques used by fraudsters is vital to fraud and compliance risk management.

Education and training are also important in connection with knowing how to utilise some of the tools that fraud investigators and those involved in detecting fraud need to know. Whether it's new developments in data analytics or any other tool that can be used, these tools are changing and improving all the time.

Even some of the characteristics of fraud risk management that one might not think change rapidly often involve changing best practices. For example, many people think the process for performing a fraud risk assessment doesn't change. Though the high-level components of what goes into a risk assessment might not change very quickly, the underlying steps often do evolve and best (or what I'd rather call better) practices emerge. If we're not engaged in ongoing education and training, we miss these emerging trends and practices, and our ability to prevent and detect fraud and noncompliance suffers.

One final point involves the indirect benefits of education and training, at least when it's done in an in-person environment like a conference or workshop. Networking with peers from other organisations is often every bit as valuable as the more formal aspects of training. Hearing what types of frauds and compliance issues others are facing and how their approaches to managing these risks are changing is the most under-appreciated aspect of attending conferences and workshops.

Tarun Bhatia

Bhatia: I am a firm believer that anything we learn today could be redundant tomorrow. Hence, there is a need for continuous education on emerging threats and means to mitigate and prevent such threats. Companies need to continuously monitor threats and inform their employees of the same. Secondly, while technology is a big influencer in corporate fraud, it is only the means to defraud. There are failures in processes and people that lead to fraud. Training of course is the easiest way to address this risk. There are three basic principles for effective training; developing content through practical examples; effective delivery of the training with easy reach to all the attendees; and high recall value to implement the learnings on the job. As an organisation, once we are able to achieve these principles, the results are generally positive and also can be easily measured. Another important aspect is to update the training content. Many organisations retain the same training material for four or five years and employees do not take it seriously and thus start ignoring the basic rules and principles. Similarly, professional investigators need to constantly upgrade their skills to ensure they offer the best and most effective solutions to their clients.

Q11. How can identity verification and fraud protection solutions be utilised to prevent illicit activities from infiltrating businesses or organisations?

Tarun Bhatia

Bhatia: Identity verification is a crucial security measure in combatting fraud, especially due to impersonation. Imagine a situation of life insurance claim being processed for an alive person, a driving license issued to a school-going child, or a bank account opened in someone else's name. Various digital solutions like face recognition, biometric verification and digital ID document verification have been used to verify identity of a person. All have various security features to prove its authenticity. We often recommend our clients for similar such verification checks in the process of onboarding employees/contractors/third parties, providing secured access. Depending on the sensitivity of the business, enhanced security features also need to be installed. Increasingly, we are seeing the use of drones in monitoring and identifying any abnormal activity. Similarly, for payments, adding additional security features ensures avoidance of fraudulent payments. Furthermore, GPS trackers linked to vehicles and individuals are actively being used in many industries to ensure there is no fraudulent loss of goods and materials.

David Schreuders

Schreuders: As described in my previous answers when discussing Trade Based Money Laundering and cash integration risk, it is paramount for companies to have an effective KYC process in place. Part of that process will be the verification of the Ultimate Beneficial Owner of the corporate the company is doing business with. It will be the basis for asking the right questions before onboarding the customer or accepting the payment, in the scope of mitigating culpable money laundering risks.

Screening of employees could also be a method for mitigating infiltration risks: it must be prohibited that forbidden relationships are established between traders and customers or third parties who are part of the criminal organisations trying to launder their proceeds of crime through legitimate trading companies. However, whether or not to screen candidates will only depend on the outcome of a specific risk assessment and is not necessary for each and every trading company.

Q12. What key technologies should companies be using to identify risks and address vulnerabilities?

Gerry Zack

Zack: My answer to this question is really a two-part extension of my answers to a couple of previous questions. Data analytics was for many years limited to structured data, the types of data that fit within the parameters of the traditional spreadsheet or database format. But it is now much easier to analyse unstructured data, such as evaluating communications, messages, explanations and other forms of text for signs of deception or other characteristics.

Additionally, artificial intelligence can be used to learn communications and other patterns in data and become quite efficient at identifying the changes in these patterns or inconsistencies that are telltale signs of fraud. We're still very much in the early stages of harnessing the power of AI as a risk identification tool. The next few years will be exciting.

And one final technology that fraud investigators should invest in relates to my previous answer regarding the difficulty in explaining and presenting complex fraud cases. Graphic depiction of data makes this task much simpler. This is part art and part science. The science part involves investing in the software that can take complex data and illustrate in a logical manner. The art part is deciding among the many different ways that the software will allow you to present the same data.

Telling the story of what happened is the final step in an investigation, and an important one that ensures all the relevant stakeholders understand all of what they need to understand. Telling complex stories using thousands of words alone may work in some instances, but it often leads to failure. Supplementing the story with charts, graphs, and other illustrations brings everything to life and leads to much greater understanding for most people who will be reading an investigative report or listening to explanations of a fraud.

David Schreuders

Schreuders: In my experience, all kinds of tools and technologies could be put in place, but at the end of the day it will all come down to people and culture – were employees trained properly, were they diligent enough and did they have the courage to speak up when coming across red flags?

CorporateLiveWire