GIR

ASIA-PACIFIC
INVESTIGATIONS REVIEW 2023

As well as daily news, GIR curates a range of comprehensive regional reviews. This volume contains insight and thought leadership from 17 pre-eminent practitioners in the Asia-Pacific region. Inside you will find articles on Australia, China and Singapore; on the main types of cryptocurrency fraud and how to trace cryptocurrency; and on how to 'do' a multi-jurisdictional internal investigations with all of challenges and contradictory requests from various agencies that those can entail.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

Contents

While reading, click this icon to jump back to the Contents at any time

Part 1: Cross-border overviews

Navigating and Preventing Cross-border Investigations 2
Weng Yee Ng, Charlie Steele and Drew Costello
Forensic Risk Alliance

Managing Multi-jurisdictional Investigations 17
Kyle Wombolt, Jeremy Birch and Christopher Clay
Herbert Smith Freehills

Part 2 Cryptocurrency

Emerging Trends in Crypto Fraud 41
Gwynn Hopkins, Akanksha Sagar and Nataliya Shokurova
Perun Consultants Limited

Sha Zhu Pan Frauds: Tracing Cryptocurrency from Nose to Tail 60
Henry Chambers
Alvarez & Marsal

Part 3: Country articles

Australia: An Increasingly Global Approach 77
Dennis Miralis, Phillip Gibson and Jasmina Ceic
Nyman Gibson Miralis

China-related Cross-border Investigation under New Data Protection Legislations 99
Gao Jun (Gary Gao)
Zhong Lun Law Firm

Singapore: Handling Financial Services Investigations 114
Joy Tan, Jenny Tsin and Ong Pei Chin
WongPartnership LLP

Preface

Welcome to the *Asia-Pacific Investigations Review 2023*, one of Global Investigations Review's annual yearbook-style reports. Global Investigations Review (for any newcomers) is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing. We tell them all they need to know about everything that matters, in their chosen professional niche.

Throughout the year, the GIR editorial team delivers daily news, surveys and features; organises the liveliest events (GIR Live); and maintains innovative research tools and know-how products to make working life more efficient.

In addition, with the aid of external contributors, we curate a range of regional reviews that go deeper into local developments than the exigencies of journalism allow.

The *Asia-Pacific Investigations Review* is one such publication. It contains insight and thought leadership from 17 pre-eminent practitioners from across the region. Across some 130-plus pages, you will find this particular volume to be part retrospective, part primer, part crystal ball – and 100 per cent useful. As you would expect from GIR, all contributors are vetted for their standing and knowledge before being invited to take part.

Together they address a variety of subjects pertinent to internal investigations undertaken in the region, complete with footnotes and relevant statistics. This edition in particular focuses on Australia, Singapore and China, and has overviews on cryptocurrencies, on the challenge of dealing with more than one national enforcement agency, and on how to work smarter in the post-covid world.

As so often with our annual reviews, a close read yields many gems. On this occasion, for this reader, they included that:

- Vietnam is on an anti-corruption drive;
- Singapore requires you to report if property may be 'connected' to crime even where the property (or the crime) are unconnected with Singapore;
- LinkedIn is one of the apps sophisticated fraudsters now use to find and groom their victims; and
- There are 18,000 cryptocurrencies currently in existence.

And much, much more. I also commend the Herbert Smith article on the challenges of multi-jurisdictional internal investigations. It is one of the most lucid explanations of the key points GIR has ever published. I was also impressed, later in the book, by the splendid explanation of the various Chinese laws conditioning data-transfer.

As ever, if you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you. Please contact us on insight@globalarbitrationreview.com.

David Samuels
Publisher, Global Investigations Review
September 2022

Part 1

Cross-border overviews

Navigating and Preventing Cross-border Investigations

Weng Yee Ng, Charlie Steele and Drew Costello

Forensic Risk Alliance

In summary

Regulatory developments impacting the Asia-Pacific and the continuing effects of the pandemic have created opportunities for new approaches to investigations in the region. Investigators who can combine global experience, local knowledge and technical expertise will have the upper hand, and the right expertise need not necessarily be the nearest. This chapter explores methods and technology that have satisfied authorities and courts in the Asia-Pacific as well as proven fraud risk mitigation efforts to avoid regulatory scrutiny.

Discussion points

- Data transfer, data management and data privacy requirements
- Document review for structured and unstructured data
- M&A related reviews
- Third-party due diligence
- Risk assessments

Referenced in this article

- The US Foreign Corrupt Practices Act and the US BIS Entity List
- The Monetary Authority of Singapore's Enforcement Report
- The *Schrems II* decision
- China's Data Security Law, Personal Information Protection Law and draft Technical Specification for Certification of Personal Information Cross-border Process
- Hong Kong's Personal Data (Privacy) Ordinance and Autonomy Act
- Japan's Act on the Protection of Personal Information
- Singapore's Personal Data Protection Act 2012

Introduction

Since the outbreak of covid-19, the world has been held hostage in more ways than one could have predicted at the start of the pandemic. Counsel and investigations experts have been forced to shift their approach to investigations in the past few years, and this necessity may ultimately have revealed more efficient, sustainable and innovative tools for resolving investigations in a manner that satisfies authorities and stakeholders in Asia-Pacific as well as those further west.

Certain trends were already evident before the pandemic: strengthening local enforcement in some countries; multi-jurisdictional matters highlighting closer coordination among authorities; and advanced technologies and remote capabilities creating new, robust and compliant ways of handling investigations across borders. These trends are likely to pick up momentum as the world finds its new normal. Investigators who can combine global experience, local knowledge and technical expertise will have the upper hand, and the right expertise need not necessarily be the nearest.

In this chapter, we look at recent regulatory developments impacting the Asia-Pacific, which may create opportunities for new approaches to investigations in the region. Within, we explore methods and technology that have withstood the authorities and regulatory scrutiny in the Asia-Pacific, as well as proven fraud risk mitigation efforts.

Overview of major developments in and affecting the Asia-Pacific region

In December 2021, the US Biden administration announced its intention to focus federal resources on anti-corruption efforts across the globe, and the Asia-Pacific region continues to see enforcement actions by the US Securities Exchange Commission (SEC). Since then, there have been several notable events reinforcing the United States' focus on fighting corruption, and in particular, within the Asia Pacific region. These events extend from the Burma Business Advisory issued in January 2022 by the US Departments of Commerce, Homeland Security, Labor, State and Treasury, along with the Office of the US Trade Representative. The advisory highlighted the risks of conducting business in Myanmar due to corruption, illicit finance and human rights abuses.[1] Additionally, a corporate enforcement action was taken against South Korean Telecom Giant KT Corporation in February 2022, in which the US SEC announced that KT Corporation would pay US$6.3 million to resolve charges that it violated

1 'Risks and Considerations for Businesses and Individuals with Exposure to Entities Responsible for Undermining Democratic Processes, Facilitating Corruption, and Committing Human Rights Abuses in Burma (Myanmar)', 26 January 2022, Accessible online.

the Foreign Corrupt Practices Act (FCPA) by providing improper payments for the benefit of government officials in Korea and Vietnam.

Authorities in the Asia-Pacific region are not sitting idle when it comes to fighting corruption either. In China, for example, the Central Commission for Discipline Inspection announced in January 2022 that it would extend its anti-corruption campaign to 'investigate and punish corrupt behaviours behind the disorderly expansion of capital and platform monopolies, and cut off the link between power and capital'.[2] Elsewhere in Asia, the anti-corruption campaign drive in Vietnam has seen a number of high-ranking Vietnamese government officials who have been kicked out of the ruling Vietnamese Communist Party (VCP), including two dismissed in June 2022 over accusations that they were involved in a US$172 million alleged bribe to supply hospitals with vastly overpriced covid-19 test kits.[3]

From a sanctions and export controls perspective, the Asia-Pacific is known to be one of the world's hotspots. In 2020 and 2021, the US intensified its use of sanctions and export controls. The EU, the UK and Canada joined the US in imposing targeted sanctions on Chinese officials over allegations of human rights violation in 2021. Fast forward to 2022, Australia, Japan, New Zealand, Singapore and South Korea joined a coalition of nations imposing sanctions against Russia on the back of the invasion of Ukraine.

In addition, the Monetary Authority of Singapore (MAS) highlighted in its Enforcement Report[4], published in April 2022 for the period July 2021 to December 2021, the strong enforcement actions taken against financial institutions (FIs) and individuals for breaches of laws and regulations administered by MAS. Key enforcement outcomes mentioned in the Enforcement Report included 2.4 million Singaporean dollars in composition penalties for anti-money laundering (AML) and counter-terrorist financing (CTF) control breaches. In the same report, MAS stated that one its enforcement priorities for 2022 and 2023 relates to 'enhancing effectiveness in pursuing breaches of corporate disclosure requirements, including through close collaboration with key regulatory and enforcement partners'.

These are but some examples of how the investigation and compliance landscape in the Asia-Pacific is constantly evolving, bringing about new challenges in navigating cross-border investigations in what is known as 'the new normal' post covid-19.

2 'China says will probe corruption behaviours behind internet platform monopolies', *Reuters*, 21 Jan 2022, accessed online.
3 Pedroletti, Brice, 'In Vietnam, the anti-corruption fight is in full swing', *Le Monde*, 28 June 2022, accessed online.
4 'Enforcement Report, July 2020 to December 2021', Monetary Authority of Singapore, accessed online.

Innovative solutions to cross-border challenges

Data transfer, data management and data privacy requirements

Data privacy and national and commercial secrecy have long been key considerations for anyone conducting investigations. Outside much of the publicised US-driven concerns around IP theft, data privacy and cyber fraud stemming from China, behind-the-scenes regulations around data transfer and data privacy are also evolving, as can be seen in the invalidation of the EU–US Privacy Shield Framework by the European Union's Court of Justice in July 2020, also known as the *Schrems II* decision. In March 2022, the European Commission and the US announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework.[5]

In another example, China passed its Data Security Law (DSL) in June 2021 and its Personal Information Protection Law (PIPL) in August 2021, where both laws impact every business operating in or doing business with China, bringing forth extensive obligations regarding processing data and potential significant penalties for non-compliance. Further developments continued in 2022 in this area, including the release of the draft Technical Specification for Certification of Personal Information Cross-border Process (the Draft Specification) in April 2022 by the National Information Security Standardisation Technical Committee (TC260) for public consultation.[6] This Draft Specification establishes the Certification Regime that is introduced by the PIPL.

Elsewhere, in Hong Kong, the country's Legislative Council passed an amendment bill on the Personal Data (Privacy) Ordinance (PDPO), which took effect from October 2021, and includes provisions specifically aimed at combating doxxing activities, namely the act of publishing private or identifying information about an individual on the internet for malicious purposes. In Japan, the Act on the Protection of Personal Information (APPI) and the Enforcement Rules for the amended APPI, came into effect in April 2022, where the amendments provided clarification on what constitutes a data breach notification and the processing standards for pseudonymised information.

Turning to Singapore, the Minister for Communications and Information and Minister-in-Charge of Cybersecurity delivered the Committee of Supply (COS) speech in Parliament, announcing that the change passed in November 2020 on the Personal Data Protection Act 2012 (PDPA), where non-compliance will attract a higher penalty of up to 10 per cent of local annual turnover for organisations whose turnover exceeds 10 million Singaporean dollars, will take effect on 1 October 2022.[7]

5 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.
6 https://www.tc260.org.cn/front/postDetail.html?id=20220429181520.
7 https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/3/speech-by-mrs-josephine-teo-minister-of-communications-and-information-at-the-ministry-of-communications-and-information-committee-of-supply-debate-on-4-march-2022.

To add to the complexity of different legislations around data transfer, data management and data privacy, we should not forget that in an increasingly complex world, the sheer volume of data is growing exponentially every year. One IDC paper projected that the entire 'Global Datasphere' will reach a mind-boggling 175 zettabytes (or 175 trillion gigabytes) by 2025.[8] As data growth accelerates at an unprecedented pace, companies and investigators alike face the unenviable task of managing and controlling this data stockpile.

Using Singapore again as an example, the country's main prosecuting body, the Attorney General's Chambers (AGC), which looks after crime and financial sector cases, announced in 2019 that it was set to launch an automated litigation analysis work platform aimed at improving efficiency in its courts and also to embrace large-scale text analysis for major evidence reviews. While it has yet to be as developed as other countries in the West, it is definitely the way forward considering the ever-expanding volume of data to be considered in cross-border investigations.

Additionally, the use of ephemeral messaging applications by employees, such as WeChat, has grown in popularity in the Asia-Pacific region. This presents challenges for employers as the visibility into such information is limited, especially if employees are conducting conversations on a personal device outside of the company's network. Data privacy and state secret laws such as those in China are additional barriers a company must consider when trying to collect information contained on such platforms and to ensure any efforts to do so comply with all local regulations.

Practical tips: review data transfer and data privacy policy

Companies should not only ensure that they have proper safeguards and governance internally, but also within all its third parties, including supply chain partners where applicable. Efforts should not stop short at just a paper compliance programme. Rather, regular reviews should be performed to ensure that the company's data transfer and data privacy policies are adhered to, and broader network penetration tests should be conducted periodically.

Practical tips: mobile solution, remote data management and air gap

There are situations where concerns over the sensitivity of the data, or the investigation matter, is heightened. These situations may stem from the need to comply with country-specific laws or managing potential reputation risks to the

8 'Data Age 2025', An IDC White Paper sponsored by Seagate, November 2018, Accessed August 2022: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

company. When dealing with such concerns during a cross-border investigation, consider the deployment of a mobile solution, where data is collected and processed in-country and also, possibly, on the client's site. This solution allows for the review of data to ensure compliance with the relevant laws and regulations prior to the transfer of data out of the respective jurisdiction.

Remote data management is another application that investigation teams should consider when handling cross-border investigations, as the entire application resides on the client site and the data management resides on a remote server or host. In addition to remote data management, the solution could be further enhanced through the building of an air gap environment for the data and the team working on the matter, which reduces the risks of access to the restricted data through a common or widely used network within the organisation.

Practical tips: information governance platform

As data continues to grow globally, the volume of data that investigation teams have to manage increases and innovative solutions should be considered for deployment to enable investigation teams to efficiently and effectively conduct their work. Investigation teams should consider the use of an AI-based information governance platform to support critical data collection and early case assessments. Examples of such platforms include innovative remote collection capabilities, which involve identifying the relevant data from multiple structure and unstructured data sources simultaneously and presenting actionable intelligence in just a matter of hours. This real-time insight and access to documents gives users the opportunity to learn and understand their data immediately, providing valuable strategic advantage for organisations during regulatory investigations.

Document review – structured and unstructured data

For certain investigative matters, investigators have to interrogate both the structured and unstructured data to find the smoking gun. Where the volume of data is sizable, it is like finding the needle in the haystack. This may mean that a large team of document reviewers is required, or a significant amount of time is required to be able to complete the document review process, both of which will have an impact on costs and investigation strategy.

Practical tips: machine learning

Machine learning is no longer a foreign term to cross-border investigation teams. Correctly deployed, it can drastically cut down the number of search term hits, which directly impacts the number of relevant documents that are required for review, resulting in a more effective investigation methodology. While this approach has been tested and accepted by regulators in certain countries, it is important to remember that technology acceptance by regulators and enforcement agencies around the world will vary significantly, even within one enforcement agency. It is crucial for investigation teams to invest the time in explaining the methodology to the regulators and enforcement agencies at the early stage of the investigation and also to demonstrate the robustness of the methodology deployed. This will allow the regulators and enforcement agencies to understand and appreciate how powerful, and effective, the application of machine learning can be in an investigation.

Practical tips: triaging data

Where structured data and unstructured data are scrutinised during an investigation, often these are done separately and in silo. This means that there is a lot of back and forth between the various teams to inform one another of their findings and incorporate those findings into their respective reviews. While this process works for small- to medium-sized investigations, it may not be effective for larger investigations as the review teams may be distributed across different offices and in various parts of the world.

Organisations should consider the use of technological solutions where the findings from structured data and unstructured data are triaged and cross applied for a cost-effective, yet robust, investigation methodology. This does not mean doing away with either or both of the structured and unstructured data reviews; rather, it enhances learnings and key findings from both types of reviews and in turn enhances the output of the investigation.

Practical tips: collection of ephemeral messaging data

Companies should develop a policy that mandates that any business-related communication takes place on company-owned devices and that such information is subject to collection where necessary. Regular training should be provided to reinforce compliance with the policy and periodic monitoring can be used as a tool to test adherence.

If an investigation arises that requires the collection of information from a personal device, consent from employees may be difficult to obtain. In light of this, the company should consider ways to obtain such consent through a targeted collection that only obtains the information relevant to the matter at hand and utilises experts to perform such work to ensure the information gathered is complete and complies with all data privacy, state secret, or other local regulations.

Mergers and acquisition related compliance reviews

Asia-Pacific has long attracted the interest of foreign investors with the abundance of opportunities and growth prospects, and the region continues to be fertile ground for investment transactions – both inbound and outbound – in 2022. The M&A frenzy in 2021 carried on into 2022, with private equity (PE) funds and investment companies achieving a record number of M&A transactions.

It goes without saying that investors need to be on the look-out for potential non-compliance with multiple laws and regulations when entering into a transaction in the region, where laws, regulations and risks are far from homogeneous from country to country. The consequences of non-compliance or a potential breach can be very costly and, as a result, make the transaction non-viable for the investors. Conducting a robust pre- and post-transaction due diligence is a must.

Practical tips: pre- and post-transaction due diligence review

Appropriate due diligence pre- and post-transaction should be performed on a timely basis in order to manage risks, including the risk of successor liability, namely the risk of acquiring a company that is already under investigation and has already violated those laws, which exposes the acquirer to potential liability based on pre-acquisition acts over which it had no control. Where possible, it is prudent to perform transaction testing to assess the accuracy of the verbal representations provided by the target and obtain a proper understanding of the target's go-to-market strategy and third parties engaged.

Third-party due diligence

Third-party due diligence has always been fundamental and the rapidly shifting supply chain landscape only heightens its importance. Basic third-party due diligence is no longer sufficient as it is increasingly important for companies to look thoroughly into existing third parties. This includes the third parties' stakeholders, and their connections, key corporate officers and employees,

other upstream and downstream providers, and so on. Transactions through intermediaries and agents continues to be a high-risk area across the global supply chain, as is ensuring that products are sourced from regions where labour or other human rights abuses are common.

This trend of vetting third parties through the environmental, social and governance (ESG) lens, has only grown in prevalence. Not only do organisations need to determine their ESG commitments, but those commitments should also be aligned to the organisation's third-party management process and programmes to demonstrate due accountability across the third-party ecosystem. Recent issuance of guidelines and probes by enforcement agencies on greenwashing reinforce the need for organisation to up their game in complying with ESG regulations.

From a sanctions perspective, with new laws introduced and frequent updates made to the prohibition lists, including the US's BIS Entity List, regular reviews should be performed on third parties to ensure that sanction rules are not breached by trading with sanctioned individuals and entities. As previously mentioned, several Asia-Pacific countries recently joined the West in taking the exceptional step of imposing significant financial sanctions as a result of Russia's invasion of Ukraine, including Australia, Japan, New Zealand, Singapore and South Korea. This increases the complexity of identifying and conducting appropriate screening on third parties. Even where the application of laws remains unclear, for example the implementation of the Hong Kong Autonomy Act, companies may want to proactively review and screen their existing clientele and supply chain to identify those potentially designated as Material Contributors, even if a precautionary step.

These days, with the wealth of information publicly available, it is unacceptable and indefensible at court to claim wilful blindness or ignorance. Regulators increasingly require companies to demonstrate that they have done their utmost to obtain and review relevant information during the third-party due diligence review.

Practical tips: tailored third-party due diligence

Without belabouring the point about screening third parties, which is a well-discussed topic over the years, this topic will continue to be an important one for all organisations. Identification of the third parties that organisations do business with, as well as the ultimate beneficial owner (UBO) of those third parties, remains a key point.

Today, there are many platforms and applications available in the market that organisations can subscribe to in order to screen third parties. It is important to remember that the sources for each of the platforms and applications are

likely to differ from one another. Some platforms may be better suited for due diligence reviews for third parties domiciled or operating certain countries, based on its sources of information, so organisations should consider what sources are most appropriate for the due diligence that they intend to conduct.

Practical tips: third-party monitoring

The data landscape is growing at a rapid rate, as referenced earlier. Organisations need to understand the universe of data created and systems leveraged, the quality of the data, and how to harness those data sources effectively. It is not about creating more data for the sake of it, but how to use existing data to perform effective third-party monitoring.

For example, where companies have existing platforms and applications that already perform some of the due diligence procedures and documentation, companies should consider how best to maximise the use of information available for an improved monitoring process, including possible system interfaces, reporting dashboards and built-in notification alerts. This type of data visualisation is a helpful way of understanding the organisation's use of third parties globally, that is, go-to-market strategy, types of risks to focus on and where (jurisdictionally), as well as ensuring timely notification of instances where an updated due diligence review is required, or where certain transactions have triggered certain red flags and the investigations or compliance team should conduct a review.

Practical tips: use of forensic science

There are innovative solutions available in the market to go beyond identifying the ultimate beneficial owner (UBO) of the third parties organisations work with, but rather places the focus on the company's products instead. For example, forensic science can be used to test products to prove their origin and verifying the products' integrity is an important one to combat, as well as safeguard against, complex supply chain issues, including forced labour and greenwashing.

Risk assessment

Periodic risk assessments conducted at least annually are now the regulators' expectation. The importance of periodic reviews to ensure appropriate consideration is given to a quickly changing global trade and regulatory landscape cannot be overstated. Used effectively, a robust risk assessment will allow management to make informed business decisions, identify and mitigate

potential non-compliance occurrences, as well as ensure the implementation of an effective compliance programme.

Practical tips: leveraging data analytics

While there is no cookie-cutter approach to risk assessment, there are innovative ways in which organisations could consider conducting, or enhancing, their risk assessment. Data analytics can be deployed to normalise and interpret responses from control and process owners. Furthermore, other data sources such as internal audit reports, substantiated investigation findings and due diligence results should be digitalised and analysed to produce and refine a comprehensive risk assessment focused on highest perceived risks.

Practical tips: integrating risk assessment and controls testing

Very often, governance, risk and compliance (GRC) tools are not always fully integrated. For example, organisations may perform a risk assessment using a separate tool or standalone methodology, and subsequently document the identified risks in the GRC tool. Thereafter, actions and regular testing required to mitigate or remediate the identified risks are performed outside the GRC tool, and the results are manually inputted into the GRC tool without a full audit trail to the underlying inputs and analysis. This tends to create challenges for investigators and compliance officers to have access to the information that allows them to fully evaluate the origin of the risk, the assessment of the risks and the effectiveness of the remediation actions.

Organisations should consider ways to interface the various systems it has within its organisations, streamline the data where possible, and invest in solutions that allow effective managing of risks and remediation actions.

Monitorships

While deferred prosecution agreements (DPAs) and monitorships are not used by regulators and enforcement agencies in the Asia-Pacific region yet, they are prosecution tools that are used regularly by western countries and have an impact on companies operating within the Asia-Pacific region. In the first half of 2022, there appears to have been a revival somewhat in the use of corporate monitorships by the US Department of Justice (DOJ), as shown in the FCPA resolutions with Stericycle, Inc and Glencore plc and related entities. This gives rise to new questions about the role of independent compliance monitors and, more importantly, whether they are back to stay.

Flipping the coin over and looking at prosecutions in the Asia-Pacific, Singapore, for example, introduced the DPA framework in 2018 and modelled after the UK's approach, allowing corporates to resolve misconduct with the Public Prosecutor for the deferral of prosecution in exchange for various conditions; however, at the time of writing, no DPAs have been entered into since their introduction.

That said, it does not mean that it is a moot point for organisations operating in the Asia-Pacific region. For companies with a US touch point, it could find itself subjected to an FCPA investigation and prosecution – Deutsche Bank, Amec Foster Wheeler Ltd, WPP, Airbus, Cardinal Health, Inc, Herbalife, Goldman Sachs Group, Inc and Goldman Sachs (Malaysia) Sdn Bhd, and Beam Suntory are examples of DPA settlements with the US, some of which involved coordinated enforcement actions with the local authorities. This increased cooperation will be coupled with a Biden Administration's increased penchant for mandating monitors as part of corporate criminal resolutions where compliance programmes are deemed ineffective

Other flashy Biden administration DOJ mandates include the following:

- Considering all misconduct by a company when determining charging decisions, regardless of whether it is similar to the instant offence.
- Mandating a company must provide the government with all non-privileged information related to all individuals involved in the misconduct (not just those whose involvement was substantial) to receive cooperation credit.
- Potentially requiring chief compliance officers (CCOs) and chief executive officers (CEOs) to certify that compliance programmes have been 'reasonably designed to prevent anti-corruption violations', a requirement that is meant to ensure that CCOs stay in the loop on potential company violations and have the appropriate resources to prevent financial crime. For multinationals, the application of such a rule will likely include sub certifications pushed down to local affiliates management including those in the Asia-Pacific.

Rest assured these mandates have caught the attention of the global compliance officer community and it will be interesting to follow the application in future settlements. What remains absolute within is the importance placed on the robustness of corporations' compliance programmes.

Practical tips – regular health check (on the compliance programme)

Organisations should conduct regular review of the organisation's compliance programme, and it is even more crucial when an organisation is under investigation or trying to reach settlement with authorities. A well-built compliance programme should not be static; rather, it should evolve to reflect how

the organisation works and the environment in which it operates. Furthermore, regulators require corporations to demonstrate that the compliance programme is sufficiently robust to detect and prevent violations of key laws and regulations the corporation is subject to.

All organisations have a sizeable volume of data available, which should be used by compliance and internal controls teams to assess the appropriateness of controls designed and the operating effectiveness of those controls. Analytics, system-driven notification and alerts, dashboards and other visuals are but some examples of solutions that should be considered in enabling effective monitoring of controls and key risk areas within an organisation, including determination of topics or subject matters, and jurisdictions of highest concern, so that appropriate resources and attention are dedicated to address those concerns. Of course, the aforementioned solutions do not remove the need to perform appropriate transaction testing to demonstrate operating effectiveness of selected controls. Instead, it helps to focus testing to areas that matter most.

Conclusion

The pandemic may have temporarily put the brakes on some of the investigations and prosecutions, but the momentum has definitely picked up. The lessons learned on conducting remote investigations during the pandemic and the innovative solutions developed will undoubtedly be put to use. As we have seen in recent legislation updates, prosecutions and settlements, investigations and enforcement actions by both Western and local enforcement agencies are on the rise – things are getting back to 'normal' – and organisations should ensure that they are prepared should they find themselves in the cross hairs.

Weng Yee Ng

Forensic Risk Alliance

Weng Yee Ng is a partner at FRA. She holds almost 20 years of experience in external and internal audit and forensic accounting. She specialises in investigations from start to settlement, evaluating and building compliance programmes, risk assessments and litigation support (both civil and criminal).

Charlie Steele

Forensic Risk Alliance

Charlie Steele is a partner in FRA's Washington, DC office. Charlie is a former senior US Treasury Department and Department of Justice official with more than 30 years of government and private-sector experience in civil and criminal compliance, investigations, enforcement and litigation matters, in a variety of industries and sectors. For the past several years he has specialised primarily in Economic Sanctions and Bank Secrecy Act/Anti-Money Laundering (BSA/AML) matters.

Drew Costello

Forensic Risk Alliance

Drew Costello is a partner at FRA based in Philadelphia, Pennsylvania. Drew specialises in the areas of Forensic Accounting and Corporate Compliance with over 20 years of experience in both professional services and industry roles.

Since 1999, FRA has worked all over the world to solve complex forensic issues for our multinational clients. We are experts in forensic accounting, multi-jurisdictional investigations, corporate compliance monitorships, disputes and arbitration, data governance and forensics, complex data analytics, e-discovery consulting, regulatory disgorgement, gain and ability to pay (ATP) calculations, compliance and risk assessment, anti-money laundering (AML) and sanctions. We support a variety of compliance monitors, advise on trans-jurisdictional data privacy and data transfer issues, and have electronic discovery expertise that augments our forensic accounting and data analytics skills.

Audrey House
16-20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 (0)20 7831 9110

www.forensicrisk.com

Weng Yee Ng
wng@forensicrisk.com

Charlie Steele
csteele@forensicrisk.com

Drew Costello
acostello@forensicrisk.com