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

Part 2 Cryptocurrency

Part 3: Country articles

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

Managing Multi-jurisdictional Investigations

Kyle Wombolt, Jeremy Birch and Christopher Clay

Herbert Smith Freehills

In summary

This chapter examines issues companies should be aware of when navigating multi-jurisdictional investigations.

Discussion points

- Structuring an investigation
- Conducting an investigation
- Dealing with regulators and law enforcement

Referenced in this article

- Financial Conduct Authority (UK)
- Financial Conduct Authority Handbook (UK)
- Department of Justice (US)
- Evaluation of Corporate Compliance Programs (US)
- Principles of Federal Prosecution of Business Organizations (US)
- Australian Securities and Investments Commission (ASIC)
- Securities & Futures Commission (Hong Kong)

A credible internal investigation should be the response when things have gone wrong in any company, especially when considering potential serious misconduct. Not only do regulators and law enforcement increasingly expect a credible investigation, but a credible investigation is also recognised as a matter of good corporate governance.

Multi-jurisdictional investigations present several challenges that create risks for companies and require careful management. This article identifies a number of those risks and outlines strategies for managing them by examining three key topics:

1. Structuring an investigation
2. Conducting an investigation
3. Dealing with regulators and law enforcement

Structuring an internal investigation

Who will conduct the investigation?

Legal privilege and independence are two key considerations when determining who should lead an investigation.

A key benefit of having the investigation led by lawyers is the legally privileged status that will often attach to the communications and work product surrounding the investigation. In many jurisdictions, the privilege will attach even when much of the primary information gathering is conducted by non-lawyers, so long as they are working under the direction of lawyers. This has been a hard-learned lesson for some corporations when the primary fact-finding was undertaken or directed by non-lawyers only to have the internal documents generated then disclosed in related private litigation.[1] But privilege is not a universally recognised concept, and even where recognised, the privilege is not absolute. In a multi-jurisdictional investigation, the question of establishing and maintaining privilege becomes more complex and must be carefully considered and managed, taking account of each jurisdiction.

Regulators expect internal investigations to be credible and a critical aspect in establishing that credibility is independence. As a Director of Enforcement at the UK FCA once remarked, 'there are many cases . . . when relying on firms' internal reports has no place.'[2] Consequently, regulators may expect to initiate their own investigations and may also expect that firms' investigations

1 See, eg, *Wultz v Bank of China,* 2015 WL 362667 (S.D.N.Y.) (granting motion to compel disclosure of internal investigation documents that were not prepared at the direction of counsel).

2 Speech by Jamie Symington, Director in Enforcement, FCA, delivered at the Pinsent Masons Regulatory Conference, 5 November 2015, available at: https://www.fca.org.uk/news/speeches/internal-investigations-firms.

are conducted by third parties to establish a sufficient degree of independence. United States law enforcement and regulators expect investigations to be 'independent, objective, appropriately conducted, and properly documented'.[3] Most crucially, a credible investigation marked by 'diligence, thoroughness and speed', together with 'timely and voluntary disclosure of wrongdoing', are crucial factors US prosecutors consider in whether to bring charges against a corporation or, when doing so, whether to recommend a reduced sentence.[4]

Outside counsel are generally perceived to enjoy greater independence than in-house counsel. Depending on the circumstances, some regulators will express opposition to in-house legal teams leading internal investigations. The argument underlying this objection is that in-house legal teams are more focused on 'circling the wagons' or 'marking their own homework' than ensuring a sufficiently independent investigation. In addition, some regulators and prosecutors take the view that, in order to avoid any potential conflicts of interest with respect to retaining regular external counsel, it is sometimes good practice for corporations to engage outside counsel they may not ordinarily hire.

The independence of the investigation team may also have consequences for the maintenance of privilege. Under US law, privilege is recognised for investigations led by in-house lawyers.[5] By contrast, under EU law, legal professional privilege does not protect in-house communications, principally because in-house lawyers are not considered sufficiently independent from their employers.[6]

It is not always necessary or proportionate to engage outside counsel. The gravity of the issues, malfeasance or conduct involved will have a significant influence on this decision. For minor conduct or risk events that do not have any potential criminal or significant regulatory consequences, it may be appropriate for a company's legal function to lead the investigation, supported by internal audit, HR or compliance. For more serious events, for instance where the conduct involves potential corruption, fraud or insider trading, it is preferable to have outside counsel engaged to direct the investigation.

Consideration should also be given to the skill sets and geographic locations needed in selecting the appropriate internal team and external experts. From an internal perspective, a multidisciplinary team drawn from legal, compliance, internal audit and the business to assist with the investigation may be appropriate. External counsel should have the geographical reach and specialist legal knowledge to support the investigation in the key jurisdictions involved.

3 United States Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, p. 16. Available at: https://www.justice.gov/criminal-fraud/page/file/937501/download.

4 United States Department of Justice, *Justice Manual §9-28.700 – The Value of Cooperation, §9-28.300 – Factors to Be Considered*, available at: https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

5 See, eg, *In re Kellogg Brown & Root, Inc.*, 2014 WL 2895939, at *3 (D.C. Cir.) (holding that 'a lawyer's status as in-house counsel does not dilute the privilege'.).

6 See case C-550/07P, *Akzo Nobel Chems. Ltd & Ackros Chems. Ltd v Comm'n, 2010* E.C.R. I-08301.

Any other external experts required, such as forensic accountants, should be retained by counsel. Consideration should be given to the purpose of the engagement, how this is documented and how the relationship and workflow is managed to ensure privilege is maintained. It is a good practice to ensure that the purpose of the third-party adviser's engagement is to assist counsel in providing legal advice to the company and to document that objective. This should take account of the potential variations in privilege regimes as they apply to the work product of external non-legal experts.

Having local in-house lawyers as part of the investigation team in each relevant jurisdiction will generally be of practical benefit. However, consideration should be given to whether in-house lawyers may have been involved in the circumstances of the conduct or risk event, even if they are not suspected of any wrongdoing. If in-house lawyers are potential key witnesses, they should be excluded from the investigation team.

It is important to establish a protocol for the conduct of the investigation and to ensure coordination among all parties involved. External counsel should be responsible for directing the conduct of the investigation and managing the flow of information. Establishing workflow protocols at the outset will help. This coordination should also establish the responsibility and protocol for facing relevant regulators to avoid confusion and maintain a consistent message. This is especially important where multiple regulators are involved, as is often the case in multi-jurisdictional investigations. While regulators in some countries may expect to hear from outside counsel, regulators in other countries may expect to hear from company management.

Care should be taken to maintain the confidentiality of the investigation in order to avoid inadvertent privilege waiver as well as to maintain the integrity of the investigation itself. Relevant information should be disseminated on a need-to-know basis.

Thought should be given to the potential need to manage interested business teams or local legal or compliance teams who may attempt to conduct their own investigations. Satellite investigations have the potential to compromise the 'legitimate' investigation as well as create unhelpful and potentially non-privileged material. This is particularly the case when satellite investigations are motivated by self-preservation, where reports generated may be biased and aim to shift blame to other parts of the business.

Who will the investigation team report to?

For the most part, this is determined by the question: who is the client? The answer will be influenced by the corporate structure as it relates to the conduct, the geographic locations the conduct touches and whether any members of senior management are potentially implicated.

Multi-jurisdictional investigations will normally only need to be carried out for multinational corporate groups. The question of which specific entity within this group should be the client will depend on how the business is structured and how this relates to the location of the relevant conduct. Although there may be a logical local epicentre of conduct, it is in most cases best to establish a regional or potentially even global level entity and their senior management as the client. This promotes independence, allows for a better management of resources and makes the process easier should more locations become involved as the investigation unfolds.

If members of senior management are potentially implicated, whether as witnesses or wrongdoers, alternatives to reporting to senior management generally need to be considered. It might be preferable for the investigating team to report to the board of directors, the audit committee or a specially constituted committee to address any potential conflict.

The location of the investigation team and any management committee may impact regulatory reporting obligations, which should be considered when establishing a reporting structure for the investigation.

Information will inevitably need to be reported to others in the organisation besides the primary report. Entities in different locations or jurisdictions will need information for the purposes of managing their businesses and to comply with relevant local regulation. The protocol for what information is shared and in what form should be considered particularly carefully in light of the implications it can have on any claim of privilege.

How will the results of the investigation be reported?

This will depend on the purpose and audience.

Where a written report is being prepared, care should be taken to maintain privilege. The distribution of the written report might need to exclude jurisdictions where privilege might be jeopardised. Fortunately, jurisdictions where privilege is not recognised or only has a less robust equivalent also tend to have a more restrictive scope for disclosure, which can mitigate to some extent the risk that the written report will be subject to a successful disclosure request.

Where a detailed written report is prepared as part of the investigation, simply sharing this among parts of the business that require some information should be avoided. Information should instead be filtered for relevance to the recipient, provided only where absolutely needed and caveated with appropriate warnings on its strict confidentiality and restrictions on further dissemination. Verbal reports should be favoured over written reports for this purpose where possible. Where extracting from or referring directly to the findings of any final report is needed, the potential implications for any claim to privilege over the detailed report should be carefully considered.

It is now common to receive requests from regulators to waive privilege and provide the report as an act of cooperation. For example, although the United States Department of Justice has expressed unambiguous support for the attorney-client privilege and clarified that 'prosecutors should not ask for such waivers and are directed not to do so' industry complaints on this issue persist in a country with a very wide array of state and federal regulators and law enforcement authorities that do not always share common approaches to enforcement.[7] Such disclosure will normally be made under a limited waiver of privilege. This involves a waiver as it applies to the regulator or law enforcement body who has agreed to maintain the report's confidentiality, but not waiving privilege as it applies to the rest of the world. Such disclosure can have benefits as an act of cooperation. Where the company's response to a conduct risk event has been exemplary, providing the report is the most credible way of evidencing that response.

The concept of limited waiver does have judicial support in many jurisdictions but the consequences of a limited waiver remain unpredictable, particularly in a multi-jurisdictional investigation.[8] There will often be a real risk that, submitting a report to one or more regulators under strict confidentiality will still result in a waiver as it applies, for instance, to third parties in subsequent private litigation. Therefore, companies must assess the benefits and risks before voluntarily disclosing any privileged document to a regulator. In the jurisdictions where limited waiver is recognised, best practice is generally to seek an explicit confidentiality agreement with any government entity when considering making a disclosure of privileged information to that entity.

7 United States Department of Justice, *Justice Manual §9-28.710 – Attorney-client and Work Product Protections*, available at: https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

8 See generally Andrew Eastwood, Providing Your Legal Advice to the Regulator, 41 *Austl. Bus. L. Rev.* 66 (2013). In the United States, industry-specific efforts to address such concerns have resulted in actual legislation, but such efforts are not universal or comprehensive. See, eg, 12 U.S.C. § 1828(x), establishing rule that the disclosure of information to federal or foreign banking regulators 'shall not be construed as waiving, destroying, or otherwise affecting any privilege such person may claim . . . as to any person or entity'.

The possibility of an investigation report being disclosed to a regulator or to a third-party litigant should be kept in mind from the beginning of any investigation. Accordingly, the purpose, content and clarity of an investigation report should be a focus for the investigation team.

Conducting an investigation

Determining the scope of the investigation

The first step is to identify the relevant events underlying the allegations. This is only possible after a preliminary investigation. In determining the scope, being proactive does not mean there is a need to 'aimlessly boil the ocean'. While in the past, DOJ officials have stated that some companies' overly broad investigations had even hindered the DOJ's efforts to resolve matters in a timely fashion,[9] more recent statements from Deputy Attorney General Lisa Monaco of the Department of Justice have clarified that it is now expected that internal investigations will identify 'all individuals involved in or responsible for the misconduct at issue' regardless of seniority in order to be eligible for cooperation credit.[10] Companies must therefore balance thoroughness with the need to satisfy evolving expectations regarding the scope of an investigation.

This must further be balanced against the need to ask: if this is happening here, is it happening elsewhere? Regulators expect that consideration should be given to different business lines and to different jurisdictions. Financial institutions involved in Libor manipulation faced criticism for failing to consider whether there may have been similar or related misconduct involving other benchmarks within the bank.[11]

Accordingly, a good internal investigation should be focused on the matter in hand and the possible compliance failings that permitted the event to occur but should also appropriately encompass possible systemic issues. This will necessarily be a balancing exercise.

More specific parameters must then be determined, such as the relevant:

- time period;
- geographic locations;

9 See Leslie R Caldwell, Assistant Attorney Gen., Dep't of Justice, Remarks at New York University Law School's Program on Corporate Compliance and Enforcement (17 April 2015) (transcript available at www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-new-york-university-law.

10 See Lisa Monaco, Keynote at ABA's 36th National Institute on White Collar Crime (28 October 2021) available at: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

11 See eg, News, UK Financial Conduct Authority, 'FCA fines five banks £1.1 billion for FX failings and announced industry-wide remediation programme' (12 November 2014), www.fca.org.uk/news/fca-fines-five-banks-for-fx-failings (last visited 27 July 2015).

- jurisdictions; and
- employees.

The relevant geographic locations and jurisdictions will not always be the same. Some laws have extraterritorial application, such as anti-corruption or financial market misconduct legislation, which may mean a jurisdiction will become relevant even though the primary misconduct occurred outside that jurisdiction's borders.

Finally, the scope of the investigation will need to be expanded if significant new issues emerge. This is not a failing of the initial scoping exercise but a reality of conducting complex investigations.

How will information be collected and reviewed?

The investigation team should identify key data sources, establishing what type of data is required and where that data is stored. Data can include communications data such as email, instant messaging logs and voice recordings as well as non-communications data such as financial records, trading records, system logs or other business documents. Data collection and processing can represent a significant challenge in multi-jurisdictional investigations, especially in light of the introduction of data protection and other laws restricting the transfer of information across borders in recent years (discussed further below). These issues need to be addressed promptly, or it can delay commencement of a thorough investigation.

In determining the scope of documents or data collection, the investigation team needs to take into account the possibility that it may receive regulatory requests at a later time whose scope might be broader than the time period, locations and employees the company identified for its internal investigation. Similarly, opting for broader extraction criteria, even if initially there is an intention to only process and review a subset, may be more efficient in circumstances where it will be difficult or costly to undertake a second extraction if the scope of the investigation expands.

Other than extraction of information held centrally on servers, consideration should be given to key employees' data stored locally on devices such as laptops, desktops, smartphones, tablets or portable hard drives. The investigation team will need to consider the company's right to access these, whether these need to be secured immediately to preserve evidence and how best to undertake this process. Where devices have not been secured promptly the company may face criticism from regulators or law enforcement should the devices later be required for a criminal investigation or prosecution.

The investigation team should also examine the organisation's document retention policies to identify when data is archived and how long it will be preserved. Processes may differ between data types and jurisdictions. Where data may be needed in future (even if it is not being extracted immediately) regular data destruction processes should be halted.

A litigation hold notice should be issued, informing all employees with access to potentially relevant data to stop the normal process of disposal of data, to not destroy any potentially relevant hard-copy or soft-copy documents and to make materials available to the investigation team. The hold notice should remind employees of the possibility of having to disclose all relevant internal documents in litigation or regulatory proceedings, which would include informal emails and chats. This can avoid the creation of unhelpful documents commenting on the conduct risk event in question. Companies should also take note that regulators are beginning to expect access to employees' private chats through messaging apps such as WhatsApp. Companies will need to carefully consider how to balance regulatory expectations and related data privacy concerns across multiple jurisdictions.

Once relevant data is preserved, the next step is the review of that data. Transfer of information across borders is often challenging, as local data privacy and state secrecy laws, as well as other blocking statutes, may impose restrictions.

The scope of state secrecy laws can be broad and ambiguous. For instance, China's state secrecy laws restrict transfer of a broad list of items that may be state secrets and include a catch-all provision for 'other matters that are classified as state secrets by the National State Secrets Bureau'.[12]

Similarly, the restrictions imposed by data privacy laws can be significant. For instance, the EU's General Data Protection Regulation (GDPR) casts a wide net in terms of what constitutes 'personal data' (ie, any information relating to an identified or identifiable natural person) and imposes onerous restrictions on its processing, transfer and security with extensive extraterritorial application. The GDPR imposes onerous obligations on the handling and processing of data, which includes transparency or notification obligations, which can present challenges in the context of investigations. Data transfers to third parties or across borders can also create difficulties. Similar restrictions to those under GDPR are imposed by the PRC Personal Information Protection Law, which came into effect more recently, in November 2021.

In addition to state secrecy and data privacy laws as outlined above, a number of Chinese laws contain provisions that may further restrict the provision or transfer of information outside China. For instance, the International Criminal

12 See Baoshou Guojia Mimi Fa (Law on Guarding State Secrets) (promulgated by the Standing Committee of the National People's Congress, 29 April 2010, effective 1 October 2010) section 9 LawInfoChina (last visited 27 July 2015) (PRC).

Judicial Assistance Law provides that organisations and individuals within the territory of China shall not provide assistance in criminal proceedings outside the jurisdiction without the approval of the competent authorities. Similar prohibitions can be found in China's Data Security Law and the Personal Information Protection Law. Companies should consider whether these laws may apply, and if so, how the risks arising from these laws can be managed.

If, having considered the local laws and regulations for the relevant jurisdictions, data cannot be transferred to the desired review location, a satellite investigation team might need to be established to review data locally with appropriate controls to ensure the review itself and the reporting of its results also do not violate local law.

The investigation team will need to develop a document review plan, accounting for the volume of data, reviewer language or other expertise necessary and how the data population can sensibly be narrowed. This will involve identifying search criteria (eg, a combination of time frame, search terms and custodians) as well as potentially more than one phase of review (eg, using less expensive resources for a first pass review). There are tools available to make the review process more efficient. Predictive coding is becoming increasingly popular in litigation but can have application in investigations as well. Predictive coding combines human review with continuous machine learning to train document review software to recognise relevant documents. Predictive coding is increasingly being embraced by enforcement authorities. In the UK, for example, the Serious Fraud Office has adopted an AI document review system that is able to recognise patterns and group information by subject, allowing the authority to deal with the increasingly vast amounts of data involved in investigations.[13]

Although predictive coding greatly increases the efficiency of the review process, even in jurisdictions where it has gained general judicial acceptance there is still uncertainty as to how and when it should be deployed in an investigations context and there is a risk that a regulator or law enforcement may take the view that a predictive coding assisted review lacks credibility.

What needs to be considered when interviewing employees?

The investigation team should identify employees they wish to interview then determine who should conduct these interviews and how these interviews should be conducted.

13 https://www.sfo.gov.uk/2018/04/10/ai-powered-robo-lawyer-helps-step-up-the-sfos-fight-against-economic-crime/ – similarly, in an enforcement outcomes report issued in December 2015, the Australian Securities and Investments Commission (ASIC) stated that it is 'increasingly adopting smarter strategies that use tools such as predictive coding, machine learning and computer algorithms' in its investigations (see paragraph 29).

The team should be mindful of the extent to which privilege covers the notes of interviews with employees. For interview notes prepared in jurisdictions where privilege is not recognised, the company may at a later stage be compelled to disclose those notes to litigants or regulators. Even in jurisdictions where privilege is recognised, the nature of the protection can differ, which needs to be considered when structuring and documenting interviews.

Steps that can be taken to protect privilege include the following:

- Having a lawyer lead or at least co-lead the interview where non-legal staff are required to conduct substantive questioning.
- Explaining to the interviewee employee that the lawyers represent the company not the interviewee, that the interview is privileged and confidential, but such privilege belongs to the company and may be waived in the future if the company wishes to disclose the notes of the interview (known as an *Upjohn* warning).[14]
- Having a designated note-taker (preferably a lawyer) who will produce the sole notes of the interview, which should be clearly marked privileged and confidential.

Where an employee is suspected to have committed an offence, depending on the law and best practice in the relevant jurisdiction, the investigation team should consider giving a specific caution to the interviewee on incriminating themselves in the interview. Aside from affording the employee procedural fairness, the failure to caution can have an impact on the admissibility of any confessions made in subsequent criminal proceedings against the individual.

In the UK, for example, guidance relating to the Police and Criminal Evidence Act states that, where a person is questioned regarding their involvement or suspected involvement in a criminal offence, then the interview must be carried out under caution and the person must be given sufficient information to enable them to understand the nature of any such offence and why they are suspected of committing it, as well as allow them to effectively exercise their rights of defence.[15]

A related issue that companies may need to confront is an employee who does not want to cooperate with an investigation for fear of incriminating themselves. In the United States, courts have found that employers may terminate employees who refuse to cooperate with an investigation even where the company is cooperating with law enforcement.[16]

14 The phrase is derived from the decision in *Upjohn Co. v United States*, 449 US 383 (1981).
15 *PACE Code of Practice – Code C, Section 11.1A.*
16 *See, eg, Gilman v Marsh & McLennan Cos.*, 286 F.3d 69 (2d Cir. 2016) (finding that an employer subject to a criminal investigation had a right to terminate an employee who refused to participate in internal

Interviewees often ask whether they can engage independent legal representation to attend any interviews with them and whether the company will pay for this. A policy for the investigation should be considered in advance, which may differ between jurisdictions depending on local requirements or practices.

The investigation team should also consider local legal and cultural issues. For instance, it may be necessary or preferable for local lawyers to lead interviews and for interviews to be conducted in the interviewee's first language. Cultural differences or language barriers may undermine the fact-finding purpose of the interview by making the employee feel uncomfortable or hesitant.

Advice from local lawyers on best practice in each jurisdiction should always be sought prior to conducting interviews. There may be relatively straightforward steps that can be taken to avoid significant collateral issues arising from interviews.

Similarly, the investigation team should understand any common risks regarding methods of undermining investigations or retaliation and seek advice on ways to mitigate these. Engaging a third-party security specialist may be necessary in particularly volatile situations or in unstable locations.

Engagement with one or more regulators may be necessary before conducting interviews depending on the circumstances. A variety of approaches can be taken by regulators or law enforcement, which includes:

- requesting that certain employees not be spoken to until the regulator has had the opportunity to interview them;
- requesting that potential wrongdoers not be alerted to the existence of an investigation until the regulator has had the chance to conduct its own further inquiries (which obviously prevents any internal interview with those individuals from taking place); or
- requiring that the interview plan or list of questions for certain employees be provided to the regulator for their review and comment prior to the interview and that the interview notes are disclosed once prepared.

What action should be taken in response to the findings of the investigation?

The two main responses to any internal investigation will be disciplining wrongdoers and strengthening policies, procedures, systems and controls.

investigation where the existence of an investigation and prosecution of alleged co-conspirators provided a reasonable basis for requesting employee's cooperation).

Even before the conclusion of the investigation, consideration should be given to whether those suspected of wrongdoing need to be suspended pending the completion of the investigation. This maintains the integrity of the investigation and minimises the risk of further issues for the company. Regulators or law enforcement may have an expectation that such action be taken or that, at the very least, increased supervision is implemented. Rights of suspension and the potential for claims of adverse action or constructive dismissal will vary between jurisdictions, so local employment law should be considered.

Similarly, although the approach to disciplining wrongdoers should ideally be consistent, employment laws and contractual variances between jurisdictions will have an impact. Regulators and law enforcement will generally expect a disciplinary outcome to be proportionate with the findings of wrongdoing. With an increasing focus on promoting an ethical and compliant culture within companies, many regulators actively discourage companies from letting wrongdoers resign quietly. However, jurisdictions with very protective employment laws may make this difficult and companies will need to carefully balance disciplinary outcomes in this respect.

The company should also strengthen any internal policies, procedures, systems or controls as soon as it is clear that such procedures and controls are found to need enhancement. Although there can be a natural hesitance to do so, given that it may be interpreted as an admission that they were inadequate, it is generally better to be proactive. Furthermore, improvements should be made where needed across all relevant locations and not just where the conduct risk event occurred.

In recent years, the US DOJ and other federal regulators have taken steps to provide companies with more specific guidance around how a corporate compliance programme should impact prosecutors' decisions around whether to prosecute. The Evaluation of Corporate Compliance Programs is an essential tool for all legal, risk and compliance teams to review in helping to benchmark their compliance programmes, particularly with respect to how federal prosecutors view the design, effectiveness, independence and function of compliance programmes.[17] Other United States and foreign regulatory authorities, including the OECD, have also taken steps to offer detailed guidance.[18]

17 United States Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, p. 16. Available at: https://www.justice.gov/criminal-fraud/page/file/937501/download.

18 See, eg, United States Department of Justice and Securities Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, available at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf; United States Department of Justice Antitrust Division, *Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations*, available at https://www.justice.gov/atr/page/file/1182001/download; OECD, *Anti-Corruption Ethics and Compliance Handbook for Business*, available at https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf. See also in the UK context https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/evaluating-a-compliance-programme/.

Dealing with regulators and law enforcement

Are any reporting obligations triggered?

Regulatory reporting obligations should be considered once a preliminary investigation has been completed. It may seem attractive to delay consideration until the conclusion of a full investigation, when all the facts are known. However, reporting obligations need to be considered much earlier and potentially revisited throughout the investigation. This is because obligations may be triggered by a mere suspicion and, once triggered, there may be a relatively short window within which reporting is required.

This is not to say that the decision to report a matter should be taken hastily. Particularly where self-reporting a breach of laws or regulations, caution should be exercised in framing the report. The potential for reports to contain damaging admissions and be used in actions against the company should be kept in mind.

There are a number of categories of reporting obligations that tend to arise and require consideration and advice where an internal investigation identifies potentially criminal conduct. These include the following:

- Licensed financial institutions in many jurisdictions will often have broad self-reporting obligations. These may include the need to self-report any material breach of financial services law or regulation by the institution or its employees. The obligation imposed on firms regulated by the UK Financial Conduct Authority is a more extreme example, which requires firms to report any matter of which the regulator would reasonably expect to be informed. More recently in Hong Kong, the SFC has required all licensed corporations to provide it with information about whether any licensed individual who leaves the corporation was under any internal investigation within six months preceding his or her departure.[19]
- Financial market participants may also be required to report any suspicious market activity (for instance transactions that may constitute insider trading or market manipulation) whether this involves an employee, a client or another market participant.[20]

19 See UK Financial Conduct Authority, Financial Conduct Authority Handbook, Section 2.1, Principle 11 (Sweet & Maxwell), available at https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html; https://www.sfc.hk/en/faqs/intermediaries/licensing/Disclosure-of-investigations-commenced-by-licensed-corporations#1F6247880B044C7D99E3B87E427121B5.

20 See, eg, UK Financial Conduct Authority, Financial Conduct Authority Handbook, SUP Section 15.10, (Sweet & Maxwell), available at https://www.handbook.fca.org.uk/handbook/SUP/15/10.html; Hong Kong Securities & Futures Commission, Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, section 12.5(f), available at https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/codes/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/Code_of_conduct-Dec-2020_Eng.pdf; Australian Securities & Investment Commission, Market Integrity Rules (Securities Markets) 2017, section 5.11, available at https://www.legislation.gov.au/Details/F2022C00607/Html/Text#_Toc106176610; 31 C.F.R. section 1023.320 (2015) (reporting duties for brokers and dealers).

- Anti-money laundering legislation will often impose a reporting obligation triggered by suspicious transactions that may be linked to criminal activity or knowledge or possession of property suspected to be the proceeds or instrument of a crime. Obligations in some jurisdictions apply to a broader class of persons and institutions than banks and other financial institutions but how wide the net is cast will vary by jurisdiction.[21]
- In some jurisdictions, there may even be an obligation to report knowledge of any serious criminal act.[22]
- Listed companies may have market disclosure obligations in certain circumstances depending on the impact the wrongdoing has on the business. For instance, companies listed on a US exchange will be required to disclose material adverse developments. A finding that serious wrongdoing has occurred that renders the company's publicly reported results materially inaccurate would be required to be disclosed.

Companies will need to consider carefully where it may have reporting obligations. This will not necessarily be limited to those jurisdictions in which the relevant conduct took place. For instance, any obligations to regulators in the company's home jurisdiction should be considered as well as any jurisdictions where the business may be impacted by the relevant conduct.[23]

An example of a very broad reporting obligation that may be unexpectedly triggered is found in Singaporean legislation.[24] The act imposes an obligation to file a suspicious transaction report where any person or corporate located in Singapore, as a result of business activities, has knowledge or a suspicion that

21 See, eg, Drug Trafficking (Recovery of Proceeds) Ordinance and Organized and Serious Crime Ordinance, (2002) Cap. 455, 29, section 25A, available at http://en-rules.sfc.hk/net_file_store/new_rulebooks/h/k/HKSFC3527_1868_VER50.pdf (H.K.); Proceeds of Crime Act, 2002, c. 29, 327–340, pt. 7, available at www.legislation.gov.uk/ukpga/2002/29/pdfs/ukpga_20020029_en.pdf (Eng.); Anti-Money Laundering and Counter-Terrorism Financing Act, 2006, 99, section 41, available at https://www.comlaw.gov.au/Details/C2015C00064/57449150-da9a-40b4-95b5-01c22781e2d0 (Australia); 12 C.F.R. section 21.11 (2015).

22 For instance, section 316 of the Crimes Act 1900 (NSW) makes it a crime where a person knows or believes an indictable offence has been committed and has information that might be of material assistance in securing the apprehension of the offender or the prosecution or conviction of the offender to fail to report that matter to the police.

23 See, eg, Hong Kong Securities & Futures Commission, Circular to Intermediaries Regarding Compliance with Notification Requirements (11 May 2015), available at www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=15EC27; ASIC regulatory Guide 176 – Foreign Financial Services Providers (March 2020) at 19(d)(iii) and 21-25, available at https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-176-foreign-financial-services-providers/; UK Financial Conduct Authority, Final Notice to Goldman Sachs International (9 September 2010), available at https://www.fca.org.uk/publication/final-notices/goldman_sachs_int.pdf.

24 See Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, (2014) Cap. 65A, 60-61, section 39(1), available at http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CompId:cccb976a-f712-0eb-b2b2-ca2bcbcc2fa6 (Singapore).

any property may be connected to criminal activity. Neither the property nor the crime is required to have any connection with Singapore.

Even where there is no strict reporting obligation, companies should consider the possibility of voluntary self-reporting where appropriate. For instance, where there is a reporting obligation in one relevant jurisdiction but not another, it may be prudent to voluntarily self-report in relevant jurisdictions concurrently with satisfying mandatory reporting obligations in others. Indeed, a company self-reporting to a regulator in one jurisdiction should anticipate that the report will become known to regulators in other jurisdictions. Early voluntary self-reporting may also be indicative of active cooperation. Whether voluntary self-reporting is advisable will very much depend on the facts and the regulatory climate of each jurisdiction.[25]

For listed companies, consideration will also need to be given as to whether and when any disclosure needs to be made to the market under periodic or continuous disclosure obligations. In addition, listed entities need to be cognisant of shareholder class action risks in respect of any disclosure decisions, including where disclosure is considered but ultimately not made. The most active jurisdictions for shareholder class action claims are the US and Australia, and a nascent area in the UK. There are significant differences between the disclosure framework and statutory class action regimes in the US, Australia and the UK, and there are nuances in how the class action risks emerge and crystallise in those jurisdictions (which are beyond the scope of this article).

In circumstances where an event is assessed but is determined not to be reportable, companies should consider documenting this decision-making process in case it is ever called into question by a regulator or class action litigant.

How do secrecy obligations impact interactions with multiple regulators?

In many jurisdictions, the involvement of any regulator will be accompanied by secrecy obligations.[26] Such secrecy obligations will restrict the extent to which the company can disclose the existence and details of regulatory inquiries

25 In the United States, the Department of Justice made permanent what had been a pilot programme directed at rewarding companies with a declination of prosecution when companies are able to meet three conditions relating to a potential violation of the Foreign Corrupt Practices Act: voluntarily disclose misconduct; fully cooperate with the government's investigation; and remediate alleged misconduct through establishment of a robust compliance programme and remediation of any ill-gotten gains: United States Department of Justice, *Justice Manual -- §9-47.120 -- FCPA Corporate Enforcement Policy*, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977.

26 For example, in Hong Kong, both the Prevention of Bribery Ordinance and the Securities and Futures Ordinance prohibit the unauthorised disclosure of enquiries and investigations carried out under the Ordinances. For example, section 30 of the Prevention of Bribery Ordinance makes it an offence for any person who knows or suspects that an investigation under the Ordinance is taking place to disclose

or investigations. In the context of multi-jurisdictional investigations, it also restricts the extent to which the company can share the fact of involvement of one regulator with other regulators. This has the potential to place companies in a difficult situation if they are asked by a regulator which other regulators are aware of or have made enquiries about the relevant conduct. It will normally be possible to get relevant regulators' approval for disclosure of an investigation to other regulators, but the discussions seeking this consent should be undertaken with great care.

What does cooperation look like?

Regulators will often have a formal policy that incentivises cooperation by making more favourable outcomes and reduced penalties available. As a general rule, cooperation does not mean simply complying with lawful requests from a regulator or law enforcement. Although guidance will vary between jurisdictions and between regulatory and law enforcement bodies, there are some common threads, which include the following:

- self-reporting the occurrence of misconduct at the earliest opportunity;
- taking the initiative to undertake a credible investigation to examine the nature, extent, origins and consequences of the misconduct;
- opening a frank dialogue with the regulator or law enforcement and providing regular and meaningful updates on the progress of the investigation;
- involving regulators or law enforcement in devising the terms of reference for a review by independent experts and in subsequent stages;
- taking appropriate remedial measures in respect of personnel involved in or bearing responsibility for the matter, including dismissal or other disciplinary actions;
- instituting necessary improvements or modifications of the firm's processes, internal controls or management structure;
- appropriately identifying and assessing compensation for those adversely affected by the misconduct (eg, customers, counterparties or other third parties) and promptly paying redress;
- making available to regulators or law enforcement the complete results of (1) the investigation into the misconduct; and (2) any review work into deficiencies in the company's processes, internal controls or management structure, including improvements made;

any details of the investigation without lawful authority or reasonable excuse, while section 378 of the Securities and Futures Ordinance requires any 'specified person' (which includes any person assisting the Securities and Futures Commission with their requests and investigations) to preserve secrecy with regard to any matter coming to his or her knowledge by virtual of his or her involvement in such requests or investigations.

- voluntarily providing significant relevant material or information to the regulator or law enforcement not directly requested and of which they might otherwise not have been aware;
- waiving legal professional privilege or surmounting any data privacy concerns that attach to any of the disclosures referred to above;
- involving senior management of the company in liaison with regulators and in overseeing the implementation of remedial measures or the payment of compensation;
- quickly agreeing to the facts with the regulators or law enforcement and actively seeking to agree a basis on which appropriate enforcement action against the company could be concluded; and
- providing intelligence useful to regulators and law enforcement that contributes to successful enforcement action against other companies or individuals involved in any misconduct.

An overarching strategy should be developed when a company is looking to cooperate with multiple regulators across different jurisdictions. Cooperation will be viewed favourably in settlement discussions with all regulators. However, the formal framework for recognition of cooperation and each regulator's history of rewarding cooperation should be taken into consideration when considering how best to approach the issue of cooperation. The incentives to cooperate and the benefit available to the company must be balanced against the need to preserve privilege and defences. Where multiple government agencies are involved, there may be varying degrees of certainty around the benefits of cooperation that needs to be considered in devising the overall strategy. The different offences and available defences that a company may face in different jurisdictions also need to be accounted for. Taking into account these complexities, the overarching strategy should strive, where possible, to take a consistent approach to cooperation.

In the United States, as noted above, Deputy Attorney General Lisa Monaco announced a policy change requiring companies to disclose all responsible individuals connected with misconduct to the Department of Justice in order to be eligible for cooperation credit. Following more recent practice at the Department of Justice to avoid a proliferation of memoranda announcing major policy changes, this shift (announced in a speech) was then incorporated into the Department's Justice Manual.[27] The Department's current position constitutes a return to the policy of the Obama administration, announced by former Deputy

27 United States Department of Justice, Justice Manual §9-28.700 – The Value of Cooperation, §9-28.300 – Factors to Be Considered, available at: https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.

Attorney General Sally Yates in the 'Yates Memorandum'.[28] The requirement of providing information about *all* responsible individuals will no doubt require enhanced cooperation and investigations broader in scope. It also represents an abandonment of a softer approach that the Trump Administration had followed and that was announced in 2018 by Deputy Attorney General Rod Rosenstein.[29] A second critical policy shift announced by Deputy Attorney General Monaco is that in making charging decisions prosecutors will now consider *all* prior misconduct, including in other countries, even conduct unrelated to the matter before the Department of Justice, and even for companies who have never been subject to Department of Justice investigation.[30] This shift may also have a marked effect on the calculus of cooperation and planning the strategy of an investigation, due in no small part to questions around the expansive meaning of 'prior misconduct'.

What are the challenges of settling with multiple government agencies?

When companies are dealing with a single regulator, there is an opportunity to influence the enforcement narrative. This process can facilitate a resolution of the matter by settlement, where the company and the regulator find common ground on what the important facts and issues are. While this is still possible with multiple regulators, it can be more difficult. Regulators will have different enforcement or regulatory cultures, as well as varying focus areas and agendas, which complicates the process and may make settlement more difficult.

Companies may also be unable to settle with all regulators concurrently. Obviously, global comfort is ideal, but this is not always possible. There is increasing coordination and cooperation among regulators but there will always be at least some complication in settlement discussions. At its worst, companies face the risk of regulatory competition: regulatory institutions or individuals wanting to make a name for themselves by breaking from the pack.[31] This risks disrupting a global settlement. Differences in settlement frameworks and the tools available to individual regulators may also pose challenges for coordination.

28 See Sally Quinlan Yates, Department of Justice, Office of the Deputy Attorney General, Individual Accountability for Corporate Wrongdoing (9 September 2015), available at https://www.justice.gov/archives/dag/file/769036/download.

29 See Rod J Rosenstein, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (29 November 2018), available at https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

30 Monaco, Keynote at ABA's 36th National Institute on White Collar Crime (28 October 2021) available at: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

31 See, eg, Liz Rappaport, Max Colchester & Damian Paletta, Regulators Seek Unity in UK Bank Talks, *Wall Street Journal* (9 August 2012), available at www.wsj.com/articles/SB10000872396390443404004577579271758685942.

To address concerns about 'piling on' and receiving multiple, overlapping fines from various civil, criminal and regulatory authorities – including overseas authorities – the US Department of Justice has instructed federal prosecutors to avoid seeking excessive or duplicative fines while nevertheless recognising the importance of coordinating parallel proceedings.[32] While this is to be done 'with the goal of achieving an equitable result', the Justice Manual pointedly notes that this level of solicitude should be predicated on the consideration of several factors including, among others, the egregiousness of a company's misconduct and 'the adequacy and timeliness of a company's disclosures and its cooperation with the Department'.[33]

Conclusion

There are a number of general observations that can be made in conclusion.

First, the legal and regulatory regimes between jurisdictions will often be inconsistent. They will clash and a perfect solution for the company's next steps will not be available. The approach adopted may need to be a compromise; attempting to walk a fine line of compliance with the two (or more) competing regimes or regulators.

Second, handling information and managing the flow of that information is important. The flow of information to different entities and across borders can have consequences under the various laws relating to data privacy, state or regulatory secrecy obligations, reporting obligations and legal privilege.

Third, an understanding of local law, business and culture is important in every jurisdiction. Investigation teams should be ready to tailor the approach taken to account for differences where this is necessary and appropriate.

Fourth, it is useful to regularly reflect on the investigation and consider the overall approach and priorities afresh. Does the scope still make sense? Is the investigation plan achieving what it sought to? Is regulatory engagement where it should be? Is anything being missed?

Last, coordination is critical. The geographic dispersion and multitude of internal and external stakeholders can make the conduct of multi-jurisdictional investigations particularly challenging.

32 United States Department of Justice, Justice Manual §1-12.100 – Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising From the Same Misconduct, available at https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings.

33 United States Department of Justice, Justice Manual §1-12.100.

* *The authors wish to thank Herbert Smith Freehills associates Frederick Good, Cynthianna Yau, Christopher Hicks, Alison Cranney and Madison Ives for their contributions to this chapter.*

Kyle Wombolt

Herbert Smith Freehills

Kyle Wombolt is the global head of Herbert Smith Freehills' corporate crime and investigations practice. He has been described by clients as 'one of the cornerstones of investigations work in Asia' and 'an exceptional lawyer'. Based in Hong Kong, Kyle has 20 years' experience in Asia and has led investigations and compliance projects in more than 40 countries worldwide. He focuses on multi-jurisdictional anti-corruption, regulatory, fraud and accounting investigations, as well as trade and sanctions issues involving multinational and major regional corporates. He has extensive experience in dealing with a broad group of government agencies and regulators in key jurisdictions in Asia, Europe, Australia and the United States.

Kyle also has a diverse range of experience in implementing anti-corruption compliance programmes for a broad range of clients, including investment banks and other financial institutions and multinational companies. He regularly advises clients on corruption risks associated with a wide range of transactions, including initial public offerings, mergers and acquisitions, and joint ventures.

Kyle is admitted to practise in Hong Kong, California and New York, and is a registered foreign lawyer in England and Wales.

Jeremy Birch

Herbert Smith Freehills

Jeremy is a partner in Herbert Smith Freehills' corporate crime and investigations practice. He represents clients in government investigations, internal investigations, regulatory enforcement, and related disputes. He also regularly assists multinationals in managing the compliance and conduct risk associated with operating in a complex regulatory environment across the Asia-Pacific. Jeremy has experience in the life sciences, mining, energy,

financial services and technology sectors. His experience includes advising on complex fraud, anti-corruption, anti-money laundering, sanctions, insider dealing, market manipulation, regulatory reporting and compliance framework assessments. Jeremy is qualified in New York, Australia and Hong Kong and has also held positions in the in-house litigation teams at US and European global investment banks.

Christopher Clay

Herbert Smith Freehills

Chris is of counsel in the Tokyo office of Herbert Smith Freehills. He has extensive experience handling internal investigations, enforcement actions, regulatory matters, and crisis management issues, including matters relating to financial crimes and markets conduct. Chris is licensed in New York and worked for several years in-house at the Mitsubishi UFJ Financial Group in New York City and Tokyo.

Herbert Smith Freehills

At Herbert Smith Freehills, we believe that helping your business get results starts with understanding your perspective, whatever your sector and wherever you operate.

As one of the world's leading international law firms, we engage with the most important challenges and opportunities facing our clients. We also know that the wealth of perspectives we bring to your business only count when applied in a truly commercial context.

Whether drawing on decades of sector focus, tapping into our 25-office global network or deploying world-renowned corporate and litigation teams, we engage with your business in depth, from New York to Sydney.

With a heritage stretching back more than 100 years as leading company advisers in two G20 nations, and a pioneering record of deploying best-in-class tech and innovative legal operations, you will be as confident turning to us for no-fuss daily results as high-stakes boardroom matters.

As a 2,600-lawyer firm boasting deep resource in the Asia-Pacific and EMEA regions, as well as a fast-growing US practice, we recognise the power of diverse thinking in delivering results, both inside our firm and within the communities in which we work.

Ultimately, our insights and our people define us.

Read more about our vision, our determination to drive diversity, inclusion and responsible business, and our ambition to redefine legal services for the digital-first age.

23rd Floor Gloucester Tower
15 Queen's Road Central
Hong Kong
Tel: +852 2845 6639

QV.1 Building
250 St Georges Terrace
Perth WA 6000
Tel: + 61 8 9211 7777

Jimu Bengoshi Jimusho
Midtown Tower, 41st Floor
9-7-1 Akasaka
Minato-ku
Tokyo 107-6241
Tel: + 81 3 5412 5412

www.herbertsmithfreehills.com

Kyle Wombolt
kyle.wombolt@hsf.com

Jeremy Birch
jeremy.birch@hsf.com

Christopher Clay
christopher.clay@hsf.com

Part 2

Cryptocurrency

Emerging Trends in Crypto Fraud

Gwynn Hopkins, Akanksha Sagar and Nataliya Shokurova

Perun Consultants Limited

In summary

Cryptocurrency – it's the hottest thing in investing. Or it was. With the values of cryptocurrencies plummeting, regulations tightening and high incidences of fraud, what can investors do to protect themselves and what are the emerging trends that we need to be aware of?

Discussion points

- What are crypto assets?
- How big is the fraud problem?
- How are investors defrauded?
- Can investors protect themselves from fraud?
- How are countries dealing with crypto regulation?

Referenced in this article

- Bill Gates v Elon Musk
- China's tough stance on crypto
- Asia regulation
- The end of Gatecoin

As crypto faces a global retreat – with many investors and exchanges facing a massive sell off and steady losses – Bill Gates's recent statement rings true: 'cryptocurrencies and NFTs are 100% based on greater fool theory'.

The Microsoft founder went on: 'I like investing in things that have valuable output. The value of crypto is just what some other person decides someone else will pay for it.'

At the other end of the debate is Elon Musk. His company Tesla accepts Dogecoin as a payment method for the purchase of some merchandise. The entrepreneur even personally continues to support Dogecoin, although recently, Mr Musk was sued for US$58 billion by a Dogecoin investor who accused him of running a pyramid scheme to support the currency.

Despite the conflicting views of these prominent personalities and entrepreneurs, regulators globally continue to be wary of cryptocurrency. Virtual assets, a broader name for cryptocurrency, are perceived by regulators as a major threat to the total stability of the financial system. Crypto's recent rapid growth, increasing scale of trading activity, high price volatility and increasing involvement of institutional investors can potentially affect financial markets and investors through the wealth effect and severe price correction.

The ease and anonymity with which crypto assets can be transferred electronically and, possibly, across borders, as compared with regulated fiat currency systems, makes them highly susceptible to money laundering or terrorist financing activities. There is also the potential risk of maintaining security, with hackers stealing currencies worth millions. 'Crypto exchanges are the frontier between the dark web and the regulated fiat world,' says Tom Keatinge, a financial crime expert at the Royal United Services Institute.

Despite the concerns, the universe of digital assets continues to multiply. There are now more than 18,000 cryptocurrencies, over 400 crypto exchanges and the global market cap of cryptocurrencies currently exceeds US$900 billion.

Below, we examine the risks associated with crypto assets, the different schemes employed to defraud investors, the challenges associated with asset tracing and the regulatory environment in the two primary Asian jurisdictions of Singapore and Hong Kong for virtual assets.

What are crypto assets?

In the absence of a legal definition like there is for securities, cryptographic assets can be described as transferable digital representations that are designed in a way that prohibits their copying or duplication. The technology that facilitates the transfer of cryptographic assets is referred to as a 'blockchain' or distributed ledger technology. Blockchain is a digital, decentralised ledger that

keeps a record of all transactions that take place across a peer-to-peer network, enabling the encryption of information. Cryptographic assets and the underlying technology provide opportunities to digitise a variety of 'real world' objects. Cryptocurrencies are the most commonly known subset of cryptoassets and are primarily used as a means of exchange, with Bitcoin being the most prominent. Today we have different kind of cryptoassets such as non-fungible tokens (NFTs), synthetic assets, stablecoins and utility tokens, among others.

The pace of development in the crypto industry has far outstripped regulators' ability to respond. With social media and online forums such as Reddit becoming the primary information source for potential investors, the potential for inexperienced investors to get burnt is high.

Due to this, consumers have limited awareness of the risks associated – and the lack of protection – for these assets. Fewer than one in 10 potential buyers of cryptocurrencies have seen official warnings about crypto, according to the United Kingdom's Financial Conduct Authority.

Unlike deposit insurance for bank depositors in the scenario of a bank's inability to pay its debts when due, losses on cryptoassets are not covered under any deposit insurance schemes by government bodies.

'It's a fraud and worse than tulip bulbs,' Jamie Dimon, CEO of JP Morgan

Over US$1 billion lost to scams

According to a recent report released by the US's Federal Trade Commission, investors have lost over US$1 billion in cryptocurrency scams between January 2021 and March 2022. More than 46,000 people have lost money in crypto fraud since the beginning of 2021, making it the leading source of payment scams. The median individual reported loss was US$2,600.

Fraudsters are attracted to cryptocurrency transactions as they are anonymous and no central bank or authority follows, traces, stops or recovers fraud as it happens. Consequently, they often use cryptocurrencies for illegitimate transactions or concealing the assets acquired through a fraud. Cryptocurrency acquisition or transaction methods may include:

- purchasing cryptocurrency through a cryptocurrency exchange;
- receiving cryptocurrency as payment for legal or illegal transactions;
- purchasing cryptocurrency for cash at a cryptocurrency ATM; and
- exchanging fiat currency for cryptocurrency through informal peer-to-peer transactions.

Cryptocurrency transfers cannot be reversed, making them difficult to trace. And most people are still unfamiliar with how crypto works. Some of the most common types of crypto scams that are prevalent and have been used to defraud people are the following.

Bogus investment scams

Since 2021, US$575 million of all crypto fraud losses reported to the FTC were about false investment opportunities. They are basically Ponzi schemes where new adopters are necessary to give artificial returns to the early adopters. Most of these schemes are advertised on social media platforms like Instagram, Facebook and WhatsApp. Limited knowledge of crypto adds to the promise of huge returns – a dangerous combination.

Fake crypto trading websites and wallets

Copies of trade websites and apps are thriving. Unfortunately, they seem quite similar to the authentic ones, and some phoney websites even rank high in Google searches, making it difficult to detect the risk. Investors may 'purchase' bitcoin using these bogus websites and applications, and even see their cash rise on bogus charts. In order to gain confidence, many services even enable people to make a 'test withdrawal', allowing you to withdraw a little sum of money. However, after trying to withdraw all of their funds, investors will realise that their funds have already gone.

Pump and Dump

'Pump and Dump' schemes occur when the perpetrators buy most of the supply of a small cryptocurrency or coin with low liquidity and small market capitalisation, promote it, often by engaging celebrities, influencers, social networks and spreading fake news. This usually drives the value of this cryptocurrency or coin up. The perpetrators who were pumping the coin will now 'dump' it. One recent cautionary story involves SQUID, the 'meme coin' cryptocurrency based on the Netflix series *Squid Game*. It was soaring one moment and then lost all its value in a major drop. The coin's creators allegedly disappeared with US$3 million obtained from investors.

Romance scams

We have recently seen an increase in 'romance scams', which all follow the same pattern: an attractive woman contacts the victim online, builds their trust, then gives tips on crypto investing, recommending a crypto trading platform with the highest return ever. Almost always, the platform is a forgery. A number of similar occurrences using the currency OEN and the sites Bitfex.pro and Bitfex.vip have been recorded in Hong Kong.

Initial coin offering (ICO)

A new cryptocurrency offering is an uncontrolled method of raising cash. Investors anticipate large profits from such ICOs and quickly join up to pay for future coins using another cryptocurrency, often Bitcoin or Ethereum (ETH), straight to the fundraiser's e-wallet. Many ICOs are completely fabricated, with phony bios of non-existent team members and technical whitepapers copied from other, legitimate cryptocurrencies. However, many ICOs failed to generate funding, while others fail entirely.

Trading platforms freezing wallets without legal grounds

We get complaints about respectable platforms that take crypto assets but subsequently lock the wallets because the trader does not follow their anti-money laundering (AML) or know-your-customer (KYC) standards. This is a murky area as AML/KYC processes typically need to be completed by the platform prior to accepting crypto money. If the money had been deposited and non-compliance with AML/KYC is cited as an excuse for wallet freezing, we believe the whole transaction should be regarded null and void and the crypto money refunded to the rightful owner.

Fake cryptocurrency exchanges

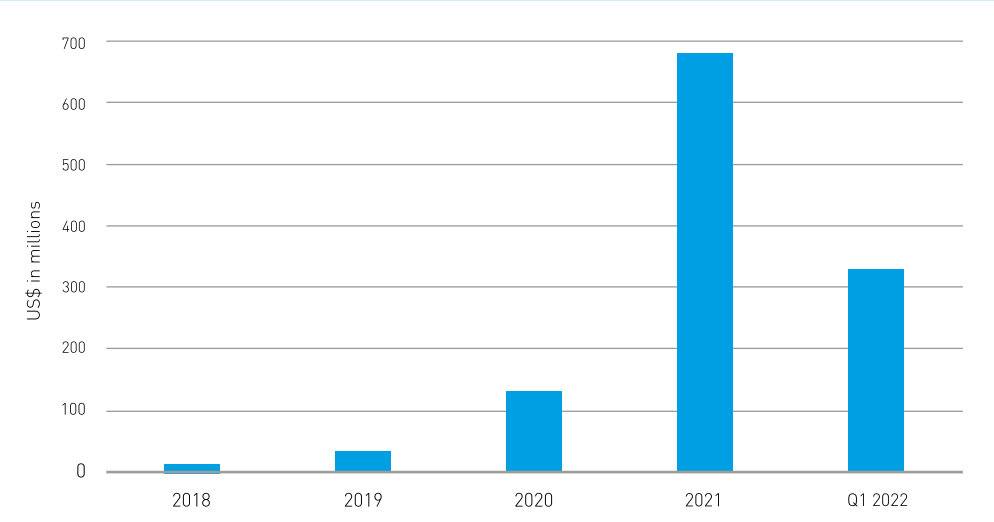
Fake and unregulated cryptocurrency exchanges act as a legitimate exchange to commit a scam. Potential victims are lured by celebrity endorsement promising extraordinary returns on investments. When a victim attempts to withdraw funds, obstacles appear such as unannounced fees and taxes to be paid. Often victims discover that their money disappears altogether. In 2017, South Korean authorities exposed one of the most notorious fake cryptocurrency exchanges. BitKRX was named to look like the cryptocurrency arm of the legitimate and largest financial trading platform in the country, Korea Exchange (KRX) — a common technique for fake exchanges trying to establish legitimacy quickly. Based on public goodwill towards KRX, BitKRX was able to lure investors

who believed BitKRX was run by KRX. But when clients who thought they had purchased BTC tried to access their funds, they discovered their money had vanished.

Fabricated cryptocurrencies

A well-known example involves the OneCoin Ponzi scheme, which defrauded victims across various jurisdictions including the United States, Europe, China and Singapore. OneCoin was an alleged form of cryptocurrency that could be mined by those who paid for educational courses and tokens that could be used to mine OneCoin. OneCoins could be exchanged for a limited amounts of fiat currency on Xcoinx (a private cryptocurrency exchange), depending on how much you had invested. In reality, no blockchain technology was involved and OneCoin was eventually discovered to be worthless.

Figure 1: Reported cryptocurrency fraud losses by year



Source: Reports show scammers cashing in on crypto craze, Federal Trade Commission, 3 June 2022. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

Weak passwords offers scope for theft

As per a recent study, 75 per cent of millennials use the same password for 10 different devices, apps and accounts and some use the same password for over 50 different sites. Blockchain wallet providers offer different security check points to prevent data hacks. Some of these include a multi-chain authentication and providing software applications such as a secured password manager. They also recommend using a VPN to access the wallet, even if using a secure Wi-Fi network. However, consumers place convenience over security making it easy for cybercriminals to attack. Cybercriminals and hackers may need just one password to gain access to a victim's crypto wallet or their complete digital

profile. Also, breach of a smartphone may provide a hacker insight into significant personally valuable data that may offer ideas about potential passwords.

Alternatively, using strongarm tactics such as kidnapping have also been used by fraudsters. In November 2021, Hong Kong Police rescued a 39-year-old cryptocurrency trader who was supposed to be attending a Tether (USDT) trade but was instead kidnapped for seven days by triad members and forced to reveal his passwords to his online banking account and cryptocurrency trading platforms, losing approximately USDT 5 million (approximately HK$39 million).

Is consumer protection possible?

How can crypto investors stay safe? Here are some key ways to protect any current or future investments.

Trustworthy internet platforms

To provide a layer of safety, cryptocurrency investors should make transactions via trustworthy internet platforms, or through legal firms rather than face-to-face. Other security strategies include maintaining strong passwords (use a trusted password manager app), spreading cryptocurrencies across different wallets, keeping the seed phrase[1] safe in an offline location, using two-factor authentication, and if technical skills allow, holding both hot and cold wallets.[2]

Public blockchains

For crypto transfers, customers should rely on public blockchains that provide visibility on all transactions taking place. With the blockchain's public ledger available and an open-source code underpinning it, it is possible to uncover associated transactions and trace the funds. Blockchain explorers can be used to undertake blockchain analysis and analyse entries for each transaction that is made.[3]

1 Seed Phrase – is a collection of 12 to 24 random words generated by a wallet service and needs to be entered in the exact same sequence as received when signing up.
2 Hot wallets can be logged into from anywhere at any time but come at a greater risk of data theft and breaches. Cold wallets are offline wallets, not connected to the internet, such as a USB device. However, if you lose your offline wallet, there is no 'forgot your password' option to recover it.
3 CFE Manual 2021, 1.1046

Crypto is NOT the new gold

When facing a too-good-to-be-true crypto scam, the best strategy is to remain wary and carry out adequate due diligence. Anybody that offers a new cryptocurrency, promising it to be a safe and high return investment without any government oversight, may not be telling the truth.

KYC requirements

Many countries now require currency exchanges – businesses that allow customers to exchange fiat currency for cryptocurrency or one cryptocurrency for another – to comply with KYC requirements or at least maintain records of customers' identities. This allows fraud examiners and legal advisers to track the money through court orders or subpoenas. Many digital wallet providers now insist on recording identifying information about their clients and this information can be used in tracing investigations.

Lack of a single jurisdiction

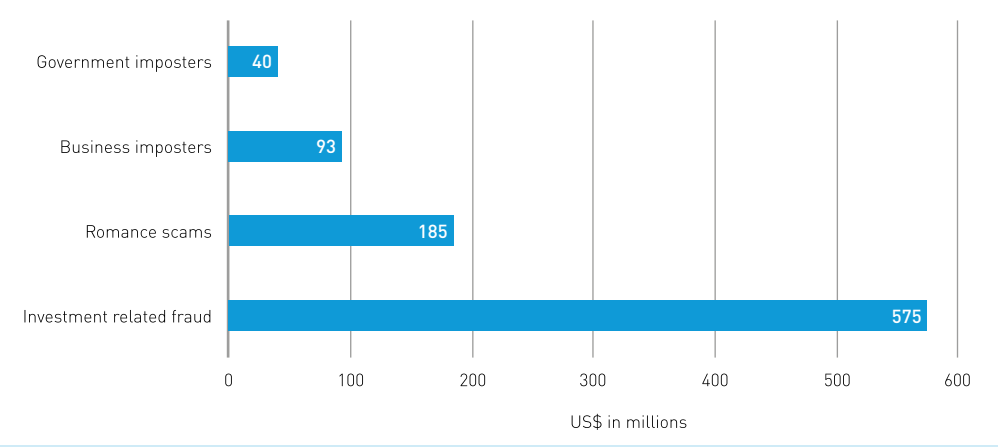
Difficulties arise when jurisdiction disclosure orders are sought and it is ambiguous which specific jurisdiction the cryptocurrency exchanges are headquartered in. For example, some of the largest cryptocurrency exchanges, such as Binance, Coinbase and Kraken do not have physical corporate headquarters.[4]

Coin mixers

Another problem with asset tracing cryptocurrencies is the use of 'coin mixers'. A coin mixer is software that allows you to break cryptocurrency into smaller amounts to be mixed with cryptocurrencies in numerous crypto wallets and then finally be deposited to the account of a choice. Such mixing of assets from various sources significantly complicates identifying and tracing cryptocurrencies.

4 https://www.businessinsider.com/crypto-startups-nix-headquarters-remote-work-coinbase-binanace-2022-5

Figure 2: Top frauds by reported cryptocurrency losses



Source: Reports show scammers cashing in on crypto craze, Federal Trade Commission, 3 June 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

Regulators are rushing to keep up

In the US, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Internal Revenue Service (IRS) have regulatory control over cryptocurrency. The IRS has taken the position that all cryptocurrency investments are assets that can be taxed like other regular assets. On 3 May 2022, the SEC announced that it was dramatically expanding its Cyber Unit and renaming it as the Crypto Assets and Cyber Unit to identify crypto fraud as a major enforcement priority.

In the UK, the Financial Conduct Authority (FCA) has alerted the public to the risks of speculation in digital assets while they work to develop standards to govern the crypto sectors. The watchdog only regulates cryptocurrency providers for anti-money laundering, but it has sent many warning signals to consumers. Since January 2020, firms carrying on cryptoassets' activity in the UK have to comply with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017. Any firms undertaking crypto asset business in the UK without registration are committing a criminal offence.

As of March 2022, the EU has also implemented new rules for the traceability of crypto assets. These include:

1. Detailing information on the source of and beneficiaries of all crypto assets, with the information available to competent authorities. Transactions from 'unhosted wallets'[5] should be included under the above rule to ensure all asset transfers can be individually identified and suspicious transactions blocked.
2. Set minimum thresholds for transactions to be eliminated and rules to cover all low value transfers.

5 A crypto asset wallet address that is in the custody of a private user.

3. A public compendium of suspicious players involved in crypto assets to be compiled by the European Banking Authority. Providers must ensure that the assets being offered are not subject to any risks of unethical activities.

Despite regulators attempts to set new guidelines and warn investors, the process hasn't been simple. The task is complicated by the large share of consumers who conduct their crypto dealing with offshore exchanges (86 per cent in the UK). A significant number of crypto businesses were not meeting anti-money laundering standards, making monitoring a struggle. With the introduction of the registration norms by the FCA in January 2020, only five companies were fully registered with until June 2021. Gary Gensler, the chair of the SEC, has said his aim was to bring 'similar protections to the exchanges where you trade crypto assets as you might expect at the New York Stock Exchange or Nasdaq'.

What about Asia?

In contrast to the western world, countries in the Asia-Pacific region have demonstrated widely differing attitudes to the regulation of crypto assets.

China's crypto shutdown

In September 2021, the People's Bank of China (PBOC) announced a total crackdown by declaring cryptocurrency an illegal tender arising from concerns over its volatility and it being misused to launder money. China joins a growing list of countries including Indonesia, Egypt and Nepal where such restrictions exist.

The restrictions have been steadily tightened over the years with the shutdown of local cryptocurrency exchanges in 2017, and trading cryptocurrency being officially banned in June 2019. The PBOC planned to block access to all forms of cryptocurrency exchanges, domestic and foreign, and Initial Coin Offering websites, although transactions continued through foreign online exchanges.

The crackdown continued with the banning of institutions and companies from providing crypto currency-related services in May 2021. Government officials warned buyers that they wouldn't receive any protection for trading in Bitcoin and other online currencies. This was followed up by payment platforms and banks being instructed to stop aiding transactions and banned the mining of cryptocurrency in June 2021.

Finally, in September 2021, all currency exchanges (both legal and virtual) engaging in information, or the buying or selling of virtual currencies were deemed illegal and carried the risk of investigation and prosecution. Financial

institutions were banned from providing services for cryptocurrencies, which included opening accounts and funds transfer. All platforms or websites providing payment services or advertising in cryptocurrencies are now banned.

China's position reflects the global concerns about cryptocurrency, such as their high-risk profile, their propensity to promote crime and their negative affect on government control of monetary systems.

What did Singapore do?

Singapore, renowned for its rigorous laws and regulations, maintains an open yet practical attitude toward cryptocurrencies. The Singapore Court recognised cryptocurrency as property and granted the first reporting freezing injunction in *CLM v CLN* [2022] SGHC 4. The city state also permits cryptocurrency exchanges and trade. Cryptocurrency players working in Singapore are regulated by the Monetary Authority of Singapore (MAS).

Singapore has robust anti-money laundering and counter-terrorism financing measures in place to stop the misuse of digital payment tokens. In the past few years, MAS introduced various AML/CTF requirements aligned with FATF standards, comprising of the introduction of the Payment Services Act (PSA), AML/CTF notice and guidelines,[6] surveillance efforts[7] and licensing and supervision. The PSA was put into effect in January 2020 by MAS, the nation's central bank and financial watchdog, to bolster consumer protection, promote trust in e-payments and improve the regulatory environment for payment services. It requires licences for crypto exchanges and other businesses involved in the cryptocurrency industry.

Since then, MAS has made a continuous effort to enhance the regulatory framework and updates to the PSA. The Singapore Parliament passed the Payment Services Bill of Amendment Act 2021. The bill will go into effect at a later date[8] and will expand the definition of a cross-border money transfer service to include facilitating transfers of funds between individuals in other jurisdictions when Singapore-based service providers are neither accepting nor receiving funds.

The Financial Services and Markets Bill mandates the licencing and compliance with regional AML and CFT regulations of digital asset providers established in Singapore but conducting business outside of the city-state. In exercising

6 Notice PS-N02 and accompanying Strengthening AML/CFT Controls of Digital Payment Token Service Providers (March 2021).

7 Surveillance efforts are concentrated on (1) identifying and discouraging DPT operations in Singapore that are not authorized and (2) using data and blockchain analytics to identify businesses that pose a larger risk.

8 The amendments made by the Amendment Act will not take effect on any certain day.

care, the MAS has also turned down applications from more than 100 Bitcoin companies looking to set up shop there.

One of the biggest cryptocurrency exchanges in the world, Binance, was told by MAS in 2021 to stop offering payment services – and courting customers – in Singapore. In order to alert Singaporean customers that the platform is neither governed nor authorised to offer payment services in the city-state, MAS also included Binance.com to its Investor Alert List in September 2021.

Subsequently, the Binance Singapore subsidiary has declared that it has withdrawn its application for a local licence and shut down its operations for digital payment tokens in Singapore.

On 14 February 2022, MAS published its Explanatory Brief on the Financial Services and Markets Bill 2022, which is currently before Parliament. If approved, this brief will allow for more stringent anti-money laundering and counterterrorism regulations for companies that provide services for virtual assets but are registered in Singapore. Any Virtual Asset Service Provider that is not already registered with MAS also falls under this.

From the above developments, it is clear that the MAS is working to facilitate rapid development in the global cryptocurrency market and that it is closely monitoring the situation to ensure that regulations are in place and risks are appropriately managed.

Crypto regulation in Hong Kong

From a jurisdiction that had minimal regulation of crypto currencies, the Hong Kong Monetary Authority (HKMA) and the SFC have gone on a fast-track mode. After concluding a consultation in May 2021, it introduced a Crypto Regulation Circular in January 2022. Under this new circular, the SFC will regulate all trading platforms that facilitate the offer, sale or purchase of any crypto in exchange for money or alternative cryptocurrency. All such agencies will be defined as 'virtual asset exchanges' and need to comply with the new AML and CTF[9] obligations. With this new rule, nearly all cryptocurrency exchanges operating in Hong Kong will need to be licensed by the SFC and offer their services to professional investors only.

9 Counter Terrorist Financing.

The Crypto Regulation Circular

This new regulation targets financial institutions, including banks and intermediaries, that wish to provide any distribution, dealing or advisory services related to cryptoassets. They also need to inform the SFC (and HKMA where applicable) in advance if they have any plans to engage in such activities. The SFC and the HKMA will grant a six-month transition period for intermediaries that have already engaged in virtual asset-related activities to adopt the new guidelines.

Virtual asset distribution services

Virtual asset-related products are considered too complex[10] and should comply with the SFC's requirements for the sale of complex products:

- Professional investors only: virtual asset-related products will only be offered to professional investors.[11] The exception is a limited suite of derivative products and funds that are traded on regulated exchanges.[12]
- Evaluation of investors: intermediaries should assess whether clients have suitable knowledge[13] of investing in virtual assets or related products prior to making transactions on their behalf. If not, necessary training needs to be provided to the clients on the nature and risks of virtual assets.
- Adequate net worth requirements and margin trading: clients should have sufficient net worth to be able to assume risks and bear potential losses of trading. This also becomes necessary in the scenario of margin calls to clients, when they have taken leverage for trading.
- KYC procedures: need to be conducted on clients dealing in virtual asset derivative products and the financial resources available for undertaking such risks.
- Due diligence: intermediaries must review products offered to the retail investors by evaluating the fund's operating parameters such as constitution, manager, custody practices, regulatory status, etc. Clients should be made aware of the product's features such as volatility, warnings on margin and deposits of the client.

10 The HKMA provides a flowchart outlining the factors to be evaluated in identifying a virtual asset-related product as a complex product.
11 The definition of a professional investor is tied to the value of a person's portfolio of cash and securities but does not include the value of any virtual assets in the portfolio.
12 These should have been specified by the SFC and should be approved for distribution to retail investors.
13 The HKMA has outlined detailed criteria for assessing whether a client has professional knowledge of virtual assets.

Virtual asset dealing services

For dealing services offered by intermediaries, the rules are more specific:

- they must be undertaken by only Type 1 – those dealing in securities – intermediaries only;
- they can only partner with SFC-licensed virtual asset trading platforms. Currently, only one exists – OSL,[14] which is operated by BC Technologies – but further approvals are in the pipeline;
- introductions to be only provided to professional investors;
- an omnibus agreement will encompass the expected conduct requirements for intermediaries such as capital requirements, KYC processes, risk control and disclosures for client trading, regular statements to client of asset portfolio, etc; and
- clients to only deposit or withdraw in fiat currency to minimise risks associated with transfer of virtual assets.

Virtual asset agency services

Similar rules, such as full compliance with all SFC and HKMA regulations and detailed conduct requirements,[15] exist for intermediaries providing advisory services in virtual assets. Detailed conduct requirements are outlined in the HKMA's circular, which specifies the following.

Guidance to banks and insurers on virtual assets and virtual asset service providers:

- Banks: the HKMA has adopted a risk-based approach to supervising banks' virtual assets activities. Banks should be cautious when lending against virtual assets as collateral and undertake additional customer due diligence and AML/CFT controls and risks. Discussions need to be undertaken with the HKMA before launching relevant virtual assets' products or services
- Insurers: insurers should be conservative and deduct the value of virtual assets in full when deriving their solvency positions. Relevant guidelines on risk management and corporate governance established by the insurance

14 OSL is a wholly owned subsidiary of BC Technology Group, a publicly listed HK entity. OSL DS (HK Limited) is the first company to be granted Type 1 & Type 7 digital asset licences by the HK SFC. OSL SG Pte Ltd. was granted licence exemption by the MAS. Its parent is Asia's only listed, 'big four' audited digital asset and fintech company providing prime brokerage, custody, exchange and SaaS services for institutional clients and professional investors.

15 HKMA details the conditions in an annexure that primarily relate to issues such as restricting services to professional investors, KYC obligations and reviewing client's financial net worth and risk appetite through a written agreement.

authority should be adhered to when designing products or evaluating risks related to virtual assets' activities.

While the regulation offers significant clarity for the regulated crypto industry servicing accredited wealthy individuals and corporations, the circular fails to account for unregulated crypto exchanges and brokers that serve retail customers. These businesses are not directly impacted by the circular, although may face competitive pressures from regulated operators. The Legislative Council will revisit the Anti Money Laundering Ordinance later this year, which will probably cover the protection of retail investors.

Liquidation of Gatecoin

Founded in 2013, Gatecoin emerged as Hong Kong's first cryptocurrency (Bitcoin and Ethereum tokens) exchange. Designed for both professional traders and retail investors, it was incubated by the Hong Kong Science Technology Parks and Tsinghua University and licenced as a Hong Kong Money Service Operator. The problems with Gatecoin started in 2016, when the exchange was the target of a security breach and lost US$2 million in cryptocurrencies (15 per cent of Gatecoin's crypto asset deposits), giving hackers access to Gatecoin's hot wallets.

According to some estimates, the market value of Bitcoin and Ethereum stolen was over US$20 million. In September 2017, Gatecoin's banking accounts with Hang Seng Bank were frozen without notice. Gatecoin unsuccessfully approached other banks and appointed a payments processor regulated by the French government.

However, the payments processor failed to process most of Gatecoin's transfers in a timely manner, while also retaining a significant portion of its funds. Despite pursuing legal action, Gatecoin was unable to recover its funds resulting in its shutdown and liquidation in March 2019. Shortly after, the SFC issued a Position Paper regarding the Regulation of Virtual Asset Trading Platforms.

Recovery of defrauded Bitcoins

The Hong Kong High Court also offered proprietary remedies to victims to recover the misappropriated Bitcoins in *Samara v Dan* (2019).[16] A judgment was handed down[17] granting relief to the petitioner for the Bitcoins transferred to the defendant and the relevant sale proceeds. It is interesting to note that some of the Bitcoins in question were sold through Gatecoin.

The plaintiff's case was that he had asked the defendant to sell 1,000 Bitcoins as an agent in return for a 3 per cent commission. Since the plaintiff was not a Hong Kong resident, the sale proceeds were to be captured in the defendant's local bank account and later transferred to the plaintiff's overseas account. However, the defendant pleaded that there was a seller and buyer relationship with the plaintiff, and he did not owe the plaintiff any money.

During the interim, a *Mareva* injunction was granted to the plaintiff to freeze the defendant's assets and a discovery order against the relevant bank account and Gatecoin to determine the underlying fund flow. Based on documents produced by the relevant bank and the liquidator of Gatecoin, the plaintiff was able to identify part of his Bitcoins and the sale proceeds.

Later at the trial, the plaintiff also produced WhatsApp communication and email records indicating the agency relationship. There was no evidence provided by the defendant denying the agency relationship or transfer of funds for the sale of some of the Bitcoins.

The court ruled that the defendant was in breach of his fiduciary duties as agent and all sale proceeds to be paid to the plaintiff. The defendant was also liable to repay the loans plus interest.

Conclusion

While crypto assets have not caused any major disruptions in Asia, market regulators are keen to ensure monetary and financial stability as these assets are increasingly adopted and evolve in complexity. As a result of covid-19, the commerce and technology sector has experienced massive transformation and development, forcing fraudsters to adapt and invent new, more sophisticated types of fraud involving cryptocurrencies.

The choices for regulators are between an opt in or pilot regime, a risk-based regime, a catch all regime or a blanket ban. While a risk-based regime is probably the preferred approach, the common objective across all jurisdictions

16 https://hsfnotes.com/asiadisputes/2022/06/23/unravelling-the-cryptic-hong-kong-court-helps-victim-recover-crypto-assets-against-pilfering-agent/.

17 https://legalref.judiciary.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=143820&QS=%28gatecoin%29&TP=JU.

is the protection of users, monetary and financial stability, minimising regulatory arbitrage, a nimble and agile regulatory framework – which efficiently accommodates the rapid market development – and financial innovation prevalent in this asset class.

Gwynn Hopkins
Perun Consultants Limited

Having previously spent 20-plus years working between Hong Kong, the Cayman Islands, the British Virgin Islands and the UK, Gwynn Hopkins founded Perun Consultants in 2017.

Gwynn has worked as an insolvency practitioner and forensic accountant on a wide range of local and cross-border engagements and has a proven track record in the liquidation and restructuring of international financial services companies, particularly those involving complex litigation or with contentious matters to resolve. Having led teams for many years as a partner in the Caribbean and Hong Kong, Gwynn has a thorough understanding of both the onshore and offshore aspects of appointments.

In addition, Gwynn has extensive experience in forensic accounting assignments including asset-tracing and recovery engagements; due diligence investigations; and the preparation of loss of profits and asset-valuation reports. Gwynn also takes roles such as acting as a consultant or an appointed independent director or trustee to assist distressed entities.

Gwynn has been recognised by *Who's Who Legal: Consulting Experts* in the fields of both forensic accounting and quantum of damages, where he is described as having 'a mind like a steel trap according to respondents, who have the utmost confidence in his views on valuation issues and methodologies'.

Akanksha Sagar
Perun Consultants Limited

Akanksha Sagar is a director at Perun Consultants.

Akanksha has an established credit background having worked for over 12 years in different roles ranging from credit ratings to distressed investing. She has significant experience in due diligence, financial analysis, business risk assessment of corporates with a focus on complex structures and distressed balance sheets. Having participated in corporate restructurings and workouts as part of the investment process, she has gained exposure to a wide range of jurisdictions in Asia.

Prior to joining Perun, Akanksha was responsible for secondary loan trading at an independent fixed income brokerage house in Hong Kong. She has also worked in Singapore where she co-headed the research team at a leading Asian distressed debt fund, and in India at GE Capital as a senior risk manager where she was responsible for GE's lending portfolio for North India.

Nataliya Shokurova

Perun Consultants (Singapore) Pte. Ltd.

Nataliya is a manager at Perun Consultants.

Nataliya spent seven years in Beijing and Shanghai where she worked in accounting both in in-house and consulting roles across various industries, including logistics, manufacturing, IT, media and entertainment, accountancy services, and F&B.

Prior to joining Perun, she served as a director of Finance & Administration for Chinese operations of a top European publicly listed IT company. A fluent Mandarin speaker, Nataliya led a team in charge of all aspects of financial and day-to-day operations.

Perun Consultants is a boutique firm with offices in Hong Kong and Singapore specialising in providing high quality services in the areas of forensic accounting, corporate advisory, restructuring, turnaround and liquidation appointments.

Perun Consultants was founded and is led by, Gwynn Hopkins, a managing director with 20-plus years of both onshore and offshore experience gained working, and having led teams for many years as a partner, in Hong Kong, the UK, the Cayman Islands and the British Virgin Islands.

7/F, Hollywood Commercial House
3-5 Old Bailey Street, Central
Hong Kong
Tel: +852 2887 8020

204B Telok Ayer Street
068640 Singapore
Tel: +65 6950 3407

www.perunconsultants.com

Gwynn Hopkins
ghopkins@perunconsultants.com

Akanksha Sagar
asagar@perunconsultants.com

Nataliya Shokurova
nshokurova@perunconsultants.com

Sha Zhu Pan Frauds: Tracing Cryptocurrency from Nose to Tail

Henry Chambers

Alvarez & Marsal

In summary

- Sha Zhu Pan frauds, or Pig Butchering frauds, are a specific fraud typology that involves the building of trust with a victim over an extended period before exploiting them for cash, often via a sham investment scheme. Such frauds have grown explosively in recent years.
- Victims of such frauds will often be walked through the acquisition of cryptocurrency before being instructed to transfer it to the fraudster. To seek recovery, a necessary step will be to trace the movement of funds to identify an entity or individual that can provide further information about the fraudster or to freeze funds.
- Tracing cryptocurrency through the blockchain is possible, but fraudsters continue to employ sophisticated techniques to obfuscate transaction flows. Such techniques include layering, chain-hopping and, most effectively, the use of tumblers.
- If a tracing exercise is successful, a victim may pursue both criminal and civil routes to recover stolen assets.

Discussion points

- Pig Butchering scams are on the rise
- Crypto-tracing techniques are needed to effect recovery

Referenced in this article

- Fangzhou Wang and Xiaoli Zhou, Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan in China, Victims & Offenders

What is a Sha Zhu Pan fraud?

Sha Zhu Pan frauds are increasing in prevalence across the globe, and are leaving thousands of unfortunate victims counting the cost of this very well-organised criminal enterprise. The phrase Sha Zhu Pan ('杀猪盘') literally translates from Mandarin to English as 'Pig Butchering'. This rather colourful term is used to describe a fraud typology whereby a fraudster (or often a syndicate of fraudsters) builds trust with a victim over weeks and months before executing the fraud to exploit the trust and extract money or other valuable assets from the victim.

It is called a pig butchering scam because the fraudster needs to invest in the scamming process. Building trust with a victim can take significant time and money — likened to the cost of raising a pig. Subsequently, once a victim has been sufficiently groomed (and in the parlance of this fraud, the pig has been sufficiently 'fattened'), then the fraud is executed, that is, cash or an equivalent is extracted from the unwitting victim.

This particular scam purportedly has its origins in mainland China, and many of the earlier incidences of this scam occurred domestically. A recent study[1] claims that, to date, nearly 60 per cent of total fraud cases reported to Chinese authorities relate to Sha Zhu Pan frauds, and the total associated loss exceeds 25 per cent of all reported fraud cases. In more recent years, however, the scam appears to be far more global, with victims being targeted internationally, including in North America and Europe. In terms of the losses per victim, it is understandably hard to quantify the dollar value. However, an online consumer rights group named Global Anti-Scam Organisation has been in contact with 1,483 Sha Zhu Pan victims worldwide and has identified US$256 million in losses, an average of US$173,000 lost per victim.[2]

The methodology used to operate and execute a Sha Zhu Pan fraud is concisely noted in a recent study:[3] 'The anatomy of the Sha Zhu Pan operation is very much like the traditional online romance scam, involving the stage of initial searching, the stage of grooming/trust-building, and the stage of financial exploitation.' The study also notes that the scammers themselves are often highly organised; much like how a business might be run; there are various departments and individuals that are responsible for performing a specific function, be that hosting the victim (ie, responsible for the day-to-day interaction), creating and maintaining the fictitious trading sites or facilitating the laundering of stolen funds.

In the fraud's most recent iteration, the use of the internet, messaging apps and social media to perpetrate the criminal activity has increased both the reach of the fraud and the value that can be extracted from the targets.

1 Fangzhou Wang and Xiaoli Zhou (2022): Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (杀猪盘) in China, Victims & Offenders, DOI: 10.1080/15564886.2022.2051109.
2 https://www.globalantiscam.org/about-us.
3 See Footnote 1.

Target identification

The first stage of a Sha Zhu Pan fraud is the identification of a target. There are many ways in which the fraudsters seek to gain a connection with an individual. Some of the more common methods include the following.

Dating apps

Dating apps such as Tinder, Bumble, Hinge, etc, can prove to be fertile hunting grounds for fraudsters. They will use fake pictures and profiles, and typically will try to move conversations from the app to other messaging platforms as soon as possible to avoid detection.

Social media

Social media sites give would-be fraudsters access to huge pools of individuals and often access to their personal data. Websites such as Facebook, Instagram and Twitter allow fraudsters to message targets directly, which, if successful, can be the starting point of the fraud. In particular, the professional social media network LinkedIn has recently been highlighted as receiving substantial attention from would-be scammers. This appears to be because fraudsters can see an individual's career history and educational background, both of which can be informative as to the likely relative affluence of the individual and therefore allow scammers to be more targeted in their approach. The risk is compounded by the fact that LinkedIn is perceived as a safe, professional networking site and that users may expect legitimate business leads to be generated through this online network. As such, inbound messages may not be treated with as much scepticism as they may otherwise be if received through a different channel. Given this, an FBI spokesperson noted in a recent interview that fraudsters who exploit LinkedIn connections for such frauds pose a 'significant threat'[4] to the platform and consumers.

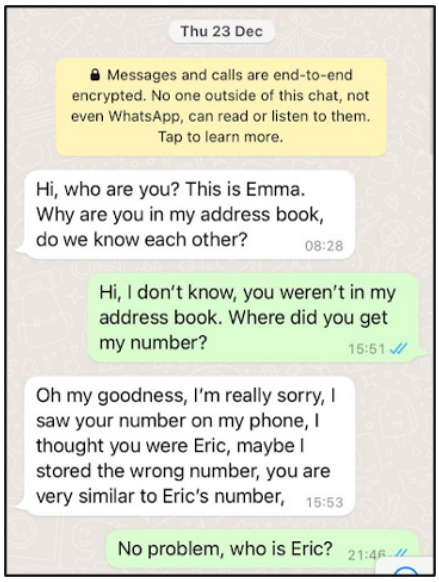
Messaging apps

Another target identification method that has been observed is the use of direct contact via messaging applications such as WhatsApp. The fraudster will send a message to the victim 'by mistake', purportedly as a result of a numerical transposition or other error. From there, the fraudster will initiate and seek

4 https://www.cnbc.com/2022/06/17/fbi-says-fraud-on-linkedin-a-significant-threat-to-platform-and-consumers.html.

to build a relationship with the victim before the next stage of the fraud. An example of this type of introductory exchange can be seen in Figure 1.

Figure 1



Source: https://www.coindesk.com/learn/crypto-romance-scams-dont-fall-for-these-dating-app-swindlers/

Building the relationship

After contact has been made by the scammer, the next step the scammer takes is to continue to develop the relationship with the individual. This is the grooming stage, where the fraudster will send messages to victims, often daily, that are based on a predefined script. Such scripts are elaborate and convincing, intending to draw the victim further into the deception. The conversation will initially focus on building a sincere relationship before turning towards a discussion of investment opportunities and, in recent examples, investment in cryptocurrency.

Executing the fraud

Once the fraudster believes they have established enough trust, they will increase the frequency and pressure on the victim to engage in a particular investment scheme. To encourage the victim to part with cash, the fraudster may offer to loan money to the individual and may even pay small amounts in 'investment profits' to build further confidence in the legitimacy of the investment.

The culmination of the fraud will be for the fraudster to extract the maximum value they can from the victim by inducing larger and larger payments into the fictitious investment scheme that will ultimately never be returned to the victim.

In addition to the 'investment' sums that are solicited, the fraudster may seek to extract other payments for fictitious taxes or fines.

Sha Zhu Pan and cryptocurrency

More generally, cryptocurrency has emerged as a further alternative conduit for fraud; the US-based Federal Trade Commission has recently estimated that the value of cryptocurrency thefts from US citizens topped US$1 billion between January 2021 and March 2022.[5] Cryptocurrency is an attractive medium for fraud due to its perceived complexity and the pseudo-anonymity that it offers. This, coupled with the explosive growth in value, growing mainstream adoption and general public curiosity, has contributed to the exponential rise of its use.

Sha Zhu Pan frauds are no different in their adoption of cryptocurrency and have moved away from forex, gold and other investments as fictitiously traded assets. In recent Sha Zhu Pan frauds, the victims are induced to invest in cryptocurrency with the promise of double-digit returns on their investment. Unfortunately, these investments are typically channelled through puppet exchange platforms controlled by the scammers and, without intervention and investigation (as described below), the victims will likely not see their cryptocurrency again.

Cryptocurrency transaction tracing

Why do we need to trace cryptocurrency?

In the unfortunate event that an individual has fallen victim to such a Sha Zhu Pan scam involving cryptocurrency, one of the starting points for recovery efforts will be to undertake a cryptocurrency tracing and investigation exercise. Such an exercise will seek to identify at a minimum:

- how the funds have moved since they left control of the victim's wallet;
- where the funds appear to have been moved to and the associated wallet addresses; and
- any transactions between the wallet addresses moving the stolen funds and identifiable wallet addresses that may hold information on the fraudster (if not the assets themselves) — for example, wallet addresses that are known to be associated with centralised exchanges.

5 https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021.

This exercise is possible as many cryptocurrencies exist on public blockchains, which allow anyone with access to the internet to view the transactions undertaken within the network as well as see balances held by a particular wallet address. This is in significant contrast to a traditional fund tracing exercise where court orders would typically be needed requiring banks to provide bank statements.

How do we start to trace cryptocurrency?

The starting point for any tracing exercise will be to identify a wallet address that is held or was funded by the victim of the fraud. In Sha Zhu Pan frauds, the fraudsters will often walk the victim through the process of acquiring cryptocurrency, and this is frequently done via a centralised exchange (eg, Coinbase or Binance). After the cryptocurrency is acquired, the funds will then typically be transferred to the first layer cryptocurrency wallet of the fraudster.

This initial on-chain transaction, moving funds from the centralised exchange to another cryptocurrency wallet outside of the exchange, can be followed on the public blockchain and would be the starting point for the investigation. To view this type of straight forward on-chain transfer, an investigator can undertake a simple transaction tracing exercise using blockchain explorer tools such as blockchain.com for Bitcoin or Etherscan.com for Ether or other ERC-20[6] tokens.

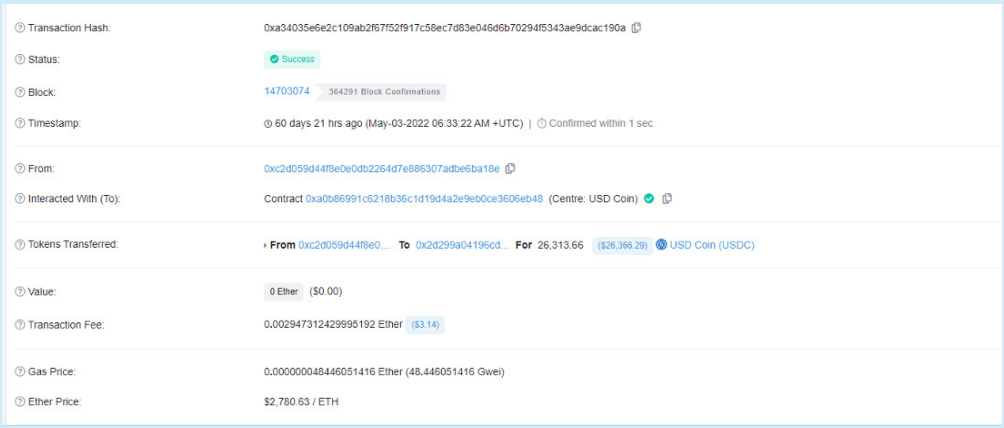
For example, an extract from Etherscan can be seen at Figure 2, which shows a transaction wherein USDC26,313.66[7] is moved from wallet 0xc2d059d44f8e0e0db2264d7e886307adbe6ba18xe to wallet 0x2d299a04196cd8335cca5711d45f5b1bc19daa0f.[8] This basic information allows investigators and tracing experts to follow the movement of tokens from wallet to wallet.

6 ERC-20 stands for Ethereum Request for Comment 20. This is a token standard that sets out certain parameters that allow for interoperability across the Ethereum network. Well known examples of ERC-20 tokens include USDC, USDT, BNB and DAI.

7 USDC is a digital stablecoin that is pegged to the USD and managed by a consortium called Centre.

8 Other information that is included in this extract shows whether the transaction has been successfully recorded on the blockchain, the transaction (gas) fees and the smart contract that the token transaction has been conducted pursuant to.

Figure 2



Why perform the tracing exercise?

The purpose of the tracing exercise is to try to identify information that could lead to the identification of the fraudster or the recovery of assets. To achieve this, an investigator will typically be looking for an exit point or off-ramp. Exit points/off-ramps are where the fraudster seeks to move the digital asset into the traditional finance world and is where they are most likely to leave a digital fingerprint that could lead to a progression of the investigation. When looking to off-ramp, there are many options available to a fraudster, but one of the most common and accessible is the use of a centralised exchange that allows digital assets to be exchanged for fiat currency.

If the digital assets can be traced to a centralised exchange, the victim and their advisers may be able to seek to freeze assets with that exchange via relevant injunctive relief, or else seek to receive further identifying information linked to the account holder that received the funds.

Obfuscating fund flows

In the case of cryptocurrency frauds, the fraudster will rarely have a simple linear transaction flow through to an exit point, and fraudsters are all too aware of the traceability of their transactions on public blockchains. As a result, they will go to great lengths to frustrate transaction tracing efforts to make the process more difficult or even impossible. Some examples of deliberate obfuscation techniques are set out below.

Layering

Layering is not a new concept and exists in the fiat currency world; it is associated with traditional frauds and money laundering. At its core, layering is the process of undertaking a series of transactions to separate the stolen funds from their illicit beginnings. Within the world of cryptocurrency, fraudsters will often move funds from wallet to wallet and comingle funds with already existing funds to obscure transaction flows.

One of the more infamous layering-type transactions within the cryptocurrency space is called a peel chain. A peel chain takes an initially large value in a cryptocurrency and undertakes numerous lower-value transactions to 'peel away' the value from the main pot. Both the smaller-valued 'peeled transaction' and the larger-valued onward transaction would typically utilise a new wallet address each time.

The peeled transactions may also be sent directly to a centralised exchange in the hope that, as the values are relatively small, they will not raise red flags. Notwithstanding, as this is a relatively common method that money launderers will employ, blockchain analytic tool providers will often seek to highlight this pattern of behaviour if it is observed, enabling the centralised exchange to react and review the transactions accordingly.

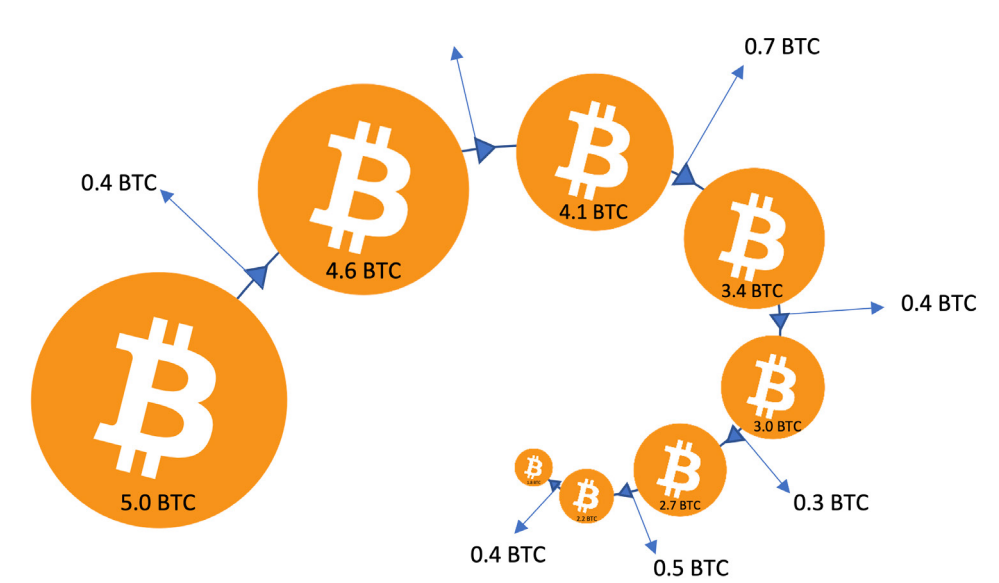
An illustration of a peel chain is provided at Figure 3 below. This diagram shows a situation where an initial wallet holding 5 BTC sends 0.4 BTC to a clean wallet,[9] and the 4.6 BTC would also be sent to a separate clean wallet.[10] The onward transaction flows continue to peel off relatively small amounts of bitcoin until almost all of the original wallet value has been dissipated. This type of layering was famously used in the 2016 hack of BitFinex (a major centralised cryptocurrency exchange) where nearly 120,000 BTC was stolen.[11]

9 A clean wallet address is an address that has not previously entered into any transactions. Such peel transactions may also be sent directly to an exchange.

10 The Bitcoin protocol works on an 'unspent transaction output' (UTXO) basis. Depending on the software wallet used, UTXO not peeled from the chain would typically be transferred to a newly created wallet address.

11 https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft.

Figure 3: Example bitcoin peel chain



Privacy coins

Not all blockchains are openly accessible, and certain cryptocurrencies have 'privacy-enhancing' features making the tracing of them considerably more difficult or even impossible. These privacy features include the use of encrypted transaction metadata, ring signatures that prevent users from identifying the true sender of a transaction and native one-time use addresses. Such cryptocurrencies are called privacy coins, and popular examples of these include Monero and Zcash.[12]

It therefore necessarily follows that such privacy coins are particularly attractive to fraudsters who are looking to hide transaction fund flows. While certain blockchain forensic tools claim to be able to visualise and trace certain privacy coins, if an investigation and tracing exercise leads to a privacy coin, it will be substantially more difficult to perform the tracing exercise.

Chain hopping and use of decentralised exchanges

The use of decentralised exchanges (DEXs) to layer the proceeds from Sha Zhu Pan frauds is particularly common and provides unique challenges to an investigator.

12 https://www.binance.com/en/blog/fiat/what-you-need-to-know-about-privacy-coins-421499824684903655.

A DEX is a cryptocurrency exchange that operates without any centralised authority managing the exchange process. It allows users to swap cryptocurrencies token for token and functions in a fully autonomous way using smart contracts to enable the exchange. Importantly, very often DEXs have little to no know-your-customer policies and procedures, allowing tokens to be exchanged anonymously.

A DEX can facilitate chain-hopping, which is a method that fraudsters can use to try to cover their tracks after having stolen illicit funds. It allows the exchange of a cryptocurrency that could fall under the control of its issuer to a cryptocurrency that cannot be restricted in the same way, or, can be 'tumbled' as described below. For example, if the fraudster receives USDT, they may want to convert that to Ether as soon as possible. This is because the issuer of the USDT may seek to freeze these tokens in a particular wallet (likely at the request of law enforcement). The conversion from USDT to Ether will also allow the fraudster to use popular tumbling protocols such as Tornado Cash, also discussed below.

The additional layering notwithstanding, if stolen tokens are moved through a DEX, it is often still possible for investigators to follow the fund flows on the blockchain, which may not otherwise be possible if they were moved to a centralised exchange (compliant or otherwise).

Use of tumblers

Probably the most popular and effective tactic that can be used by scammers to make the tracing of the cryptocurrency flows more challenging is the use of cryptocurrency tumblers.

What is a tumbler?

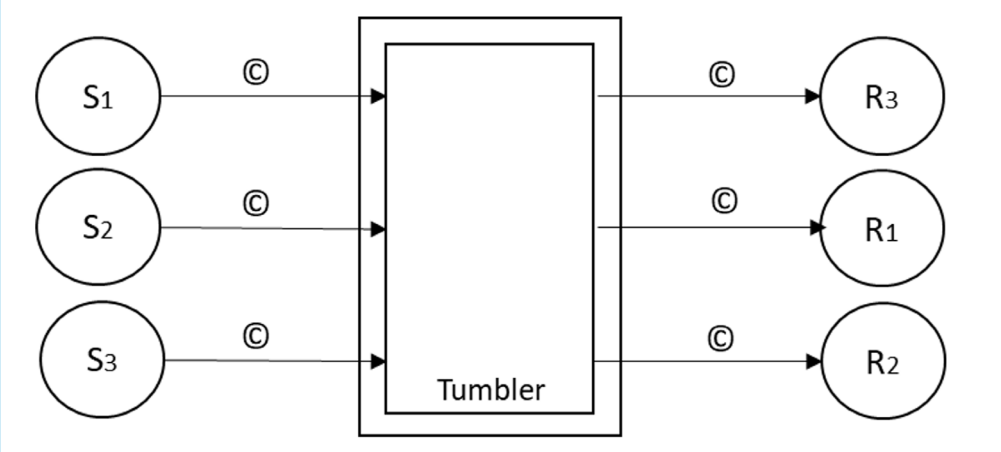
A tumbler is an online cryptocurrency service that is used to obscure a transaction trail from a sender (S) to the receiver (R) by mixing cryptocurrencies from other senders into a pool before then distributing the cryptocurrencies to the designated receiver(s).

For example, in a simple transaction as shown at Figure 4, it is clear that R_1 received one unit of cryptocurrency from S_1.

Figure 4

However, when a tumbler is used, it is much harder to establish linkages between the incoming and outgoing funds with a high degree of confidence, Figure 5.

Figure 5



As the tokens being moved through a tumbler are necessarily fungible, without knowing the instructions provided by the user, an investigator will not be able to identify exactly which input token (Sender) relates to which output tokens (Receiver).

Centralised and decentralised tumblers

There are two types of tumblers; centralised and decentralised. As with centralised and decentralised exchanges, the primary difference between the two is that centralised tumblers are owned and controlled by individual parties, while decentralised tumblers are autonomous and are controlled only by the code of the smart contracts and protocols by which they interact.

Although a centralised tumbler is easier to set up and administer, the level of anonymity it provides is limited by the fact that law enforcement agencies can seize the transaction records. Such record seizure would allow the matching of inputs and outputs and, therefore, a continuation of the transaction graph.

An example of such a seizure occurred in May 2019 when European authorities seized BestMixer.io, a centralised Tumbler. Law enforcement successfully secured information, including IP address, transaction logs, wallet addresses and chat messages from the seized servers.[13] This occurred even though BestMixer.io claimed that the order history was automatically and permanently destroyed 24 hours after the execution of the order.[14]

13 https://www.ccn.com/europol-ends-crypto-bestmixer-200-million-bitcoin-laundering/.
14 https://bestmixer.pro/.

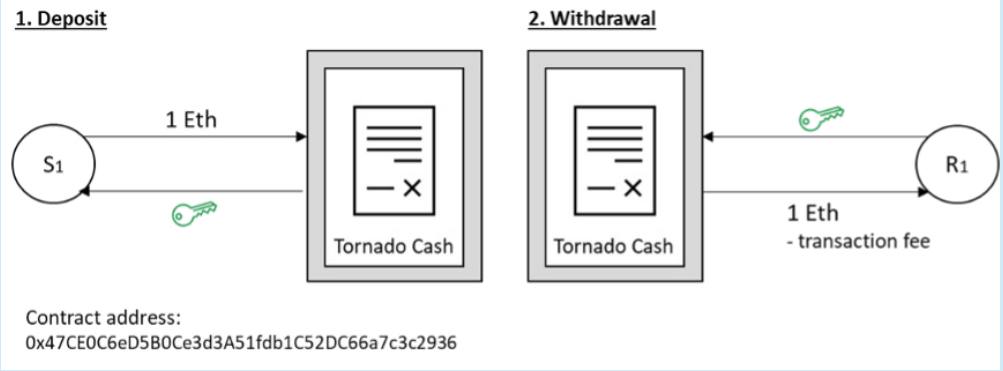
Decentralised tumblers offer a trustless tumbling service by using smart contracts, which are programmes that will run automatically according to the defined rules when predetermined conditions are met. Such tumblers may be preferred by those looking to use tumbler services, as they do not need to trust individuals or entities; rather, they need only trust the code on which the tumbling protocol is based.

Example of a decentralised tumbler – Tornado Cash

Tornado Cash[15] is one of the most popular decentralised tumblers on the Ethereum network. It allows users to deposit cryptocurrency to a smart contract that gives them an encrypted note (similar to a private key). Using the encrypted note, the user can subsequently withdraw the funds to a specified Ethereum wallet address.

The Tornado Cash smart contracts also limit each deposit and withdrawal to a fixed amount of cryptocurrency (eg, 0.1 Eth, 1 Eth, 10 Eth and 100 Eth), which further anonymises the transaction flow.[16] By doing so, for example, all deposits and withdrawals interacting with Tornado Cash: 1 Eth smart contract are all either depositing or withdrawing 1 Eth.

Figure 6



At the time of the deposit, the user is not required to specify the destination address for withdrawal, and there is no time limit to withdraw the funds that will be held in a liquidity pool within Tornado Cash. It is at the discretion of the holder of the encrypted note to decide when to withdraw the cryptocurrency. In general, the deeper the pool, and the longer the time the users wait to withdraw the funds, the higher the level of anonymity.

15 Note that since the drafting of this article, Tornado Cash has been added to the OFAC Sanctions list and may no longer be as popular a choice for token tumbling.

16 By having standardised smart contracts, deposit and withdrawal amounts cannot be matched by virtue of their value (eg, If we saw 1.233522 ETH being deposited and then exactly the same amount being withdrawn, we would have much greater confidence in linking this input and output).

In addition to the high level of anonymity that the tumbler already affords, upon withdrawal from Tornado Cash, the option of using a relayer is also provided. When Ethereum is withdrawn from the tumbler, a transaction fee is required to be paid from the wallet receiving the Ethereum. If the wallet is a new clean wallet, it needs to be funded to pay these transaction fees. This therefore would require the wallet to be funded by the tumbler user, which in turn may cause some level of de-anonymisation. To fix this, Tornado Cash implemented the concept of a relayer that acts as a third party to manage the entire withdrawal.

Tracing cryptocurrency through Tornado Cash

When looking to perform an investigation and tracing exercise when Tornado Cash is used, the encrypted note would be the most important key to the transaction trail. Tornado Cash allows people to use the encrypted note to generate a compliance report showing the deposit and withdrawal records, including the transaction time and the wallet addresses. However, in the context of a Sha Zhu Pan fraud, it is very unlikely that an investigator will have access to this key, so other investigation options must be considered.

Blockchain heuristics

In the absence of other information, blockchain heuristics can be used to seek to link inputs to a tumbler with outputs from a tumbler.

Blockchain heuristics are essentially shortcuts/problem-solving techniques that use other information within the blockchain to deduce insights. It is important to note that such heuristics cannot be exclusively relied upon and do have significant limitations; however, when augmented with other investigation techniques, blockchain heuristics can be a useful tool.

For example, if an investigator was performing a transaction-tracing exercise that led to a tumbler, they may look to employ heuristics to continue their transaction tracing efforts, identifying the tumbler outputs that correspond with the inputs. The investigator would first look to identify all of the outputs from the tumbler as recorded in the blockchain — If the funds have been moved out of the tumbler,[17] then this group of transactions will include those funds that the investigator is looking to trace.

17 This is a significant assumption, and it is possible that the fraudster may keep funds within a tumbler's liquidity pool.

In this scenario, a very basic heuristic that could be used to identify the onward fund flow is to disregard all output transactions that have timestamps occurring before the input timestamps. Other more advanced heuristics that may enhance an investigator's understanding of the output include:

- Total value of outputs v inputs – output addresses that receive greater amounts than the input addresses deposited are less likely to be related.
- Commonality in receipt of tumbler outputs – if two addresses receive an output from a tumbler, and then the first address subsequently sends funds to the second, we can assume that these two addresses are under common control.
- Common neighbouring addresses – if two addresses receive an output from a tumbler, and both subsequently move funds to a common third address, we can assume that all three of these addresses are under common control.
- Detour errors – transactional links between any of the tumbler input addresses and subsequent output addresses would demonstrate links between input and output addresses.

This list is not exhaustive, and other heuristics may be used or developed based on the specific information available and bespoke to the tracing scenario.

After the tracing exercise

If the investigator of the Sha Zhu Pan fund flow has successfully managed to identify a wallet address that appears to be linked to an exit point as defined above, the next steps can be assessed.

The options available to the victim will typically include:

- working with law enforcement to advance seizure efforts as well as pursue the fraud's perpetrators;
- consider with counsel potential targets for civil proceedings to freeze funds or pursue those services or entities that have facilitated the movement of the stolen funds; and
- consider with counsel potential targets to obtain information on the real identity of the fraudster.

What happens if you or your clients have been scammed?

If, unfortunately, an individual does become the victim of a scam, there are certain initial steps that should be taken. Such steps are also recommended by the team at the consumer awareness site, Global Anti Scam:[18]

- report the scam to the relevant local authorities, law enforcement or regulator in the jurisdiction that you are in;
- contact the bank or cryptocurrency exchange that facilitated the transfer so they are made aware;
- undertake a wallet and transaction tracing exercise to identify the movement of the stolen funds; and
- speak with specialist counsel or investigators to understand what the next steps in a potential recovery may be, given the circumstances specific to your case.

Henry Chambers
Alvarez & Marsal

Henry Chambers is a senior director with Alvarez & Marsal's disputes and investigations team in Hong Kong, specialising in fraud, corruption and regulatory investigations.

Henry Chambers brings over 10 years of experience in investigative accounting and disputes. His primary areas of concentration are forensic accounting and investigation assignments, fraud, corruption and regulatory matters as well as commercial litigation. Mr Chambers has worked with clients across a range of industries, including manufacturing, technology and commodities.

Most recently at Alvarez & Marsal, Mr Chambers has been involved in a cross-border investigation where he was responsible for assisting a US-headquartered manufacturing company in its internal review of potential FCPA violations in Asia. The matter involved the collection, review and analysis of accounting data, review of supporting documentation, performance of investigative interviews and preparation of findings reports for counsel.

18 https://www.globalantiscam.org/post/things-to-do-after-you-got-scammed.

When Tony Alvarez and Bryan Marsal joined forces in 1983, it was with the intent of seamlessly linking operations, performance improvement and value creation to best help companies turn areas of stagnation into growth to achieve sustainable results. This ethos remains at the core of our firm.

We are the consulting firm known for asking tough questions, listening well, digging in and rolling up our sleeves. We are fact-driven and action-oriented. We move our clients forward, to where they need to be. We are A&M.

What we do

Uncover and implement the right solution, at the right time, in the right way.

A&M provides global leadership, problem solving and value creation for companies across industries and around the world. We work as advisers, interim leaders and partners who tell you what you need to know, not always what you want to hear.

How we help

Rapid diagnosis, exacting action, practical solutions and on-site leaders.

Complex problems, shifting demands and tumultuous business environments make today's high stakes even more dangerous. Our operational heritage helps us decipher your challenges, as our commitment to value creation identifies new opportunities. Always at the ready, we stand with you.

4/F, St. George's Building
2 Ice House Street
Central, Hong Kong

alvarezandmarsal.com

Henry Chambers
hchambers@alvarezandmarsal.com

Part 3

Country articles

Australia: An Increasingly Global Approach

Dennis Miralis, Phillip Gibson and Jasmina Ceic

Nyman Gibson Miralis

In summary

This article considers the major Australian government investigative, law enforcement and regulatory agencies involved in domestic and transnational investigations, with a particular focus on their increasing need to adopt a global approach to adequately protect Australians from criminal threats, both local and international. The article examines the new internationalised mindset of Australian law enforcement, the effects of globalisation and the increased level of international collaboration between government agencies, as well as the tools and techniques utilised by such agencies to address the increasingly complex and 'borderless' nature of investigations.

Discussion points

- Background to the internationalisation of Australia's approach to the investigation of crime
- The Australian government's role in driving international coordination in the Asia-Pacific region and globally

Referenced in this article

- National Strategy to Fight Transnational, Serious and Organised Crime
- The Australian Federal Police, including its international work
- Other examples of inter-agency collaboration, including the Commonwealth Director of Public Prosecutions Organised Crime and Counter-Terrorism Practice Group, the Serious Financial Crime Taskforce, the Pacific Transnational Crime Network and the United Nations Office on Drugs and Crime Regional Programme for Southeast Asia and the Pacific
- The Mutual Assistance in Criminal Matters Act and Extradition Act
- The Australian Sanctions Office

Introduction

In the past, Australian government investigations were primarily focused on individuals and corporations operating within Australia's borders. Globalisation, however, has led (and continues to lead) to Australian government agencies' increasing involvement in cross-border investigations, often working collaboratively with their international counterparts in parallel investigations. One of the main drivers of this change has been the internationalisation of commerce and the subsequent increase in 'borderless crimes', such as money laundering, tax evasion, e-commerce fraud, corruption, bribery, cybercrime and terrorism financing.

This article surveys the major Australian government agencies involved in such investigations, their capabilities and involvement in transnational investigations, and recent examples of the execution of such investigative capacities. The article takes a particular focus on the increasing need to adopt a global approach to adequately protect Australians from criminal threats, both local and international.

National Strategy to Fight Transnational, Serious and Organised Crime

In December 2018, the Minister for Home Affairs announced the launch of the National Strategy to Fight Transnational, Serious and Organised Crime (TSOC), an agreement signed by the Council of Australian Governments. Building on the insights of the 2017 Australian Foreign Policy White Paper, the National Strategy to fight TSOC is a collaborative government response to the damage caused to Australian citizens by transnational crime typologies, such as the trade of illicit drugs, money laundering, cybercrime and child sexual exploitation.

Such examples of serious criminal activities are generally perpetrated by sophisticated and well-resourced criminal groups. The Australian government has responded by further development of existing law enforcement capabilities onshore and abroad. In addition to the development of existing Australian law enforcement agencies, the National TSOC Strategy promotes an increased level of inter-agency collaboration.

The initiative represents an integrated and formalised national framework to combat TSOC and guide commonwealth and state governments.

The Australian Federal Police (AFP) states that key partnerships and initiatives include: international engagement (ie, cooperation with a range of international partners to disrupt crime at its source overseas); government engagement (ie, building partnerships across governments, domestically and internationally, to enhance collaborative relationships across intelligence, law enforcement, border management, justice, legal, education, health and social policy agencies,

to ensure a multifaceted response to the threat posed by TSOC); private sector, civil society and academic engagement (ie, to help to build a strong understanding of the threats and environment, and raise awareness, promote vigilance and emphasise the importance of combating TSOC); and community engagement (ie, increasing the resilience of communities and protecting vulnerable individuals against TSOC).

The Australian Federal Police

The AFP is Australia's national law enforcement policing body, tasked with enforcing the Commonwealth criminal law, which includes the offences of foreign bribery, cybercrime, tax evasion, terrorism financing and money laundering.

The AFP states, in its report *International Engagement: 2020 and Beyond*, that the purpose of its international engagement is 'to take the fight against crime offshore, and to protect Australians and Australia's national interests by working in partnership with state, territory and foreign law enforcement agencies to detect, deter, prevent and disrupt crime at its point of origin or transit'. This represents a significant shift in the AFP's approach, which was previously focused on detecting, deterring, preventing and disrupting onshore criminal activities.

According to the report, the following statistics reflect the need for the AFP to engage with international law enforcement agencies: around 70 per cent of Australia's serious criminal targets live overseas or have links to overseas jurisdictions; fraud is said to cost Australia more than AU$6 billion each year; cybercrime costs more than AU$2 billion annually, and with changing technologies and automation this will only increase; the global cost of crime is about AU$3 trillion, and this will continue to grow; and there has been a 120 per cent increase in terrorism incidents globally since 2010.

In accordance with this evolving approach, the AFP works with global law enforcement and intelligence partners such as Interpol and the Five Eyes intelligence alliance, as well as global non-law enforcement such as the United Nations and foreign governments, to further investigations where Australian interests are affected.

The AFP: its global investigative footprint and internationalist policy

Additionally, the AFP's International Operations has strategically placed liaison officers, police advisers and missions in five regions across the globe, each with a regional manager. These regions are: the Americas; Asia; Europe, Africa and the Middle East; the Pacific and External Territories; and South East Asia.

According to the AFP, the international operations portfolio assists the AFP in the disruption of crime offshore through: disruption of transnational serious and organised crime (including terrorism); security and stabilisation missions to achieve regional stability and contribute to global order; international engagement and liaison; and capability development missions and activities.

The AFP describes its increasing internationalist approach to investigations by referencing the following three principles:

- *collaboration: brokering collaboration with international law enforcement agencies to drive investigations and support bilateral or multilateral cooperation;*
- *intelligence gathering: collecting and exchanging criminal intelligence in support of international law enforcement efforts; and*
- *capacity building: enhancing the capacity and the capability of international law enforcement agencies to combat transnational crime.*

Confirming this approach, in 2015, the AFP and FBI signed a memorandum of understanding (MOU) that focuses on the collaboration between the two agencies in addressing terrorism, illicit drugs, money laundering, illegal firearms trafficking, identity crime, cybercrime and transnational economic crime.

The MOU, called 'Combating Transnational Crime, Combating Terrorism and Developing Law Enforcement Cooperation', formalises the AFP and Federal Bureau of Investigation (FBI) cooperation in the exchange of information, resources, and technical and forensic capabilities.

The AFP has signed similar memorandums with many other countries, and additionally relies on Europol and Interpol for assistance with its investigations.

The AFP's international collaborations and operations came to the fore when, in June 2021, it was announced that the covert Operation Ironside had resulted in the over 200 arrests and the laying of over 500 criminal charges, mostly related to transnational and serious organised crime. Operation Ironside focused on the encrypted messaging app 'ANoM', and involved collaboration with the FBI, as well as over a dozen other countries' law enforcement agencies, including New Zealand and member states of Europol. It was initially reported that over 800 arrests were carried out as part of the global cooperation in this operation (known internationally as Operation Trojan Shield).

In December 2021, Phase 2 of Operation Ironside was launched, which involved a protracted offence targeting up to 160 targets around Australia including outlaw motorcycle gangs, Italian organised crime, illicit drug distributors and trusted insiders. Likely to last for months, phase 2 focuses on making arrests and disrupting criminals' business operations. Specifically, data retrieved from the AnoM platform has led to the AFP gaining significant insight into the 'Ndrangheta, their profits, their links to motorcycle gangs, and mapping the familial relationships involved. Aided by new powers under the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021, which created three new types of warrants to be applied by the AFP or the ACIC during investigations involving online activity (data disruption warrants, network activity warrants, and account takeover warrants), in June 2022 the AFP announced that a particular focus on Italian organised crime has already identified 51 Italian organised crime clans in Australia and a number of 'Ndrangheta have been charged.

The Australian Sanctions Office (ASO) in the Department of Foreign Affairs and Trade (DFAT)

Nestled within DFAT's Regulatory Legal Division in the Security, Legal and Consular Group, the ASO is Australia's sanctions regulator. The ASO provides guidance to regulated entities including government agencies, individuals, businesses and other organisations on Australian sanctions law. It also provides proactive educational services, including conducting outreach, training seminars, and publishing online information. The ASO also publishes the DFAT Consolidated List of sanctioned persons and entities, promoting compliance and helping prevent breaches of the law.

The ASO also processes applications for, and issues, sanctions permits, for individuals and entities needing to undertake activities that would otherwise be illegal under Australian sanctions laws and regulations.

The ASO works in partnership with other government agencies to monitor compliance with sanctions legislation, including AUSTRAC, the Department of Defence, Department of Home Affairs, the ABF, and the AFP, and to respond to possible breaches.

There are two types of sanctions implemented by the Australian government:

- United Nations Security Council (UNSC) sanctions, which Australia must impose as a member of the United Nations; and
- Australian autonomous sanctions, which are imposed as a matter of Australian foreign policy.

Both UNSC sanctions and Australian sanctions impose sanction 'regimes', which are usually described by reference to a country or group. In early 2022, the Australian government imposed an autonomous sanctions regime focusing on a range of individuals, companies, organisations and officials supporting Russia's invasion of Ukraine. The sanctions measures imposed in a sanctions regime focus usually on:

- restrictions on trade in goods and services;
- restrictions on engaging in commercial activities;
- targeted financial sanctions (including assets freezes) on designated persons and entities; and
- travel bans on certain persons.

A recent example of enforcement of Australian sanctions laws is the case of Chan Han Choi, who in 2021 pleaded guilty to conduct contravening the UN Charter Act and the Sanctions Act by providing brokering services for the sale of arms and related material, tactical inertial measurement units and refined petroleum products to North Korea in 2017. Satisfied that Choi's conduct was deliberate and motivated by a desire to undermine the sanctions imposed on North Korea, the Supreme Court of NSW sentenced him to three years and six months' imprisonment.

AUSTRAC and the Asia-Pacific Group on Money Laundering

AUSTRAC is Australia's anti-money laundering (AML) and counter-terrorism financing (CTF) regulator, and the specialist financial intelligence unit (FIU) responsible for identifying threats and criminal abuses in the financial system. AUSTRAC's powers are set out in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and the Financial Transactions Reports Act 1988 (Cth).

AUSTRAC primarily receives and analyses financial information, and the resulting financial intelligence is disseminated to revenue, law enforcement, national security, human services, and regulatory and other partner agencies in Australia and overseas.

By identifying potential money laundering and terrorist financing cases, AUSTRAC plays a vital role in helping partner agencies to detect money laundering and terrorist financing activity, investigation of financial crimes (including tax evasion) and securing prosecutions. This supports the protection of Australia's security, the apprehension of criminals and the protection of the integrity of Australia's financial markets.

As a result of the transnational nature of money laundering and terrorism financing, AUSTRAC is an active participant in the coordinated global response to these phenomena and therefore engages in a two-way exchange of information and intelligence with other FIUs all over the world. The information shared relates to financial transactions, financial intelligence and AML/CTF. These methods of cooperation assist international counterparts with their AML/CTF regulation and also help law enforcement agencies track the international movements of proceeds of crime.

MOUs are presently in place between AUSTRAC and 95 equivalent national FIUs, as well as three other-classified instruments of exchange. This includes successful agreements signed with prominent regional partners, such as the China Anti-Money Laundering Monitoring and Analysis Centre on 2 November 2016 and the United States counterpart, Financial Crimes Enforcement Network on 27 September 2018.

More recently, in 2022, AUSTRAC responded to the ASO's imposition of Russian sanctions by establishing a dedicated intelligence team to monitor and triage financial reporting about Russian sanctions, including suspicious matter reporting and international funds transfer reporting. This reporting is being used to produce actionable financial intelligence to assist the ASO and the AFP in detecting sanctions evasions. AUSTRAC is also part of international efforts to coordinate effective financial intelligence sharing to combat sanctions evasion, and is part of the Russia-Related Illicit Finance and Sanctions (RRIFS) FIU Working Group, a coordinated effort to track the movement of funds around the world and to identify opportunities to jointly target individuals and entities subject to sanctions, paying close attention to the abuse of shell companies and other corporate structures, and the use of third countries, to distance sanctioned persons and entities from their assets.

The most basic requirement for the dissemination of information to international partners is for the CEO of AUSTRAC to be satisfied, in accordance with section 127 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), that:

> *the foreign government requesting the information has provided requisite undertakings as set out in section 127(1)(a) of the Act; and it is appropriate to release the information in all the circumstances.*

AUSTRAC also works in conjunction with the following:

- The Financial Action Task Force (FATF) – an intergovernmental body focused on combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. In May 2020,

the FATF released the 'COVID-19 related Money Laundering and Terrorism Financing: Risks and Policy Responses' report, detailing the emerging threats of covid-19 crime typologies and best practices and policy responses for governments addressing vulnerabilities arising from the global pandemic. Additionally, in July 2021, FATF released a report titled 'Opportunities and Challenges of New Technologies for AML/CTF', considering the implications of developments in areas such as artificial intelligence and application programming interfaces.

- The Egmont Group of Financial Intelligence Units – made up of FIUs and providing a global network for enhancing cooperation among FIUs, especially in the areas of information exchange, training and the sharing of knowledge and expertise. Beyond AUSTRAC, notable Asia-Pacific (APAC) members include:
    - Hong Kong SAR, China Joint Financial Intelligence Unit;
    - Indonesian Financial Transaction Reports and Analysis Centre (PPATK); and
    - Anti-Money Laundering Office Thailand.
- The Asia/Pacific Group on Money Laundering (APG) – the FATF-style regional body for the Asia-Pacific region.

The APG consists of 41 member jurisdictions, 11 of which are also permanent members of the FATF. These core members are Australia, China, Hong Kong, the United States, Canada, Japan, Korea, Singapore, Malaysia, India and New Zealand. All members of the APG commit to implementing the international standards against money laundering set out in the recommendations of the FATF. The APG mutual evaluations or 'peer review' process involves site visits conducted by rotating teams consisting of APG legal, financial, and law enforcement experts. These teams attend upon the jurisdiction of fellow APG members for the purpose of testing their levels of technical compliance with AML standards, as set by the FATF, as well as AMF/CTF effectiveness. Twenty-five reports were generated by the third round of the APG mutual evaluations process, between 2015 and 2019.

Australia is a permanent APG co-chair. The current joint co-chair is occupied by Malaysia. The secretariat offices of the APG are located in Sydney, Australia.

Commonly, AUSTRAC will liaise with international law enforcement bodies and agencies regarding the traceability of proceeds of crime. AUSTRAC also provides extensive technical assistance and training programmes throughout the APAC region to strengthen the effectiveness of counterpart FIUs. Formal training programmes focused on capability building have been administered in

Thailand, Nepal, Indonesia, Bangladesh, Cambodia, the Philippines and Papua New Guinea. Notably, AUSTRAC has officers located in Jakarta, Kuala Lumpur, Guangzhou, London and Washington, DC.

Of particular concern to international law enforcement is the proliferation of Bitcoin and other cryptocurrency transactions, which are considered to be used in many instances for illegal purposes. The anonymity that exists in the cryptocurrency realm is what makes it difficult for law enforcement agencies to identify and track users.

Under the amendments to the Anti-Money Laundering and Counter-Terrorism Financing Act, which came into effect in 2018, AUSTRAC now monitors all digital currency exchanges within Australia's borders with the aim of ensuring that the transactions are not being used for money laundering or terrorism-related activities. AUSTRAC does this by requiring all digital currency exchange providers operating in Australia to register with AUSTRAC and meet the Australian government's AML/CTF obligations. Digital currency exchange providers have to collect information to establish a customer's identity, monitor transactional activity, and report to AUSTRAC transactions or activity that is suspicious or involves amounts of cash over AU$10,000. As a result of the legislative amendments, digital currencies are treated in the same way as physical cash in a bank with regard to money laundering and activities suspected to be linked to terrorism financing.

Any company caught operating an unregistered digital exchange will be held criminally liable. The penalties start at a two-year jail term or a fine of AU$111,000 for failure to register, and range up to seven years in jail; and, for more serious offences, a AU$2.22 million fine for corporations or a AU$444,000 fine for individuals. The use of this legislative framework enhances the ability of the Australian government to more comprehensively investigate emerging crimes, such as money laundering through the use of cryptocurrency, as well as cybercrime, on an international scale.

The Australian Criminal Intelligence Commission

The Australian Criminal Intelligence Commission (ACIC) is Australia's national criminal intelligence agency with 'specialist investigative capabilities'. The ACIC is the only agency in Australia that is exclusively focused on combating serious and organised crime.

The ACIC's remit for 'specialist investigative capabilities', working with domestic and international partner agencies, involves:

- collecting, correlating, analysing and disseminating criminal intelligence and combining it to create a comprehensive national database;

- using coercive powers (similar to a Royal Commission) to obtain information where traditional law enforcement methods have not been effective;
- providing strategic intelligence assessments and advice; and
- implementing a national target management framework to guide law enforcement in establishing and sharing organised crime priorities and targets. This is particularly useful for dealing with multi-jurisdictional serious and organised crime investigations.

The Australian Security and Investments Commission

The Australian Security and Investments Commission (ASIC) exercises its powers under the Australian Securities and Investments Commission Act 2001 (Cth) (ASIC Act) to regulate many aspects of Australia's corporate, market and financial sectors. ASIC possesses the discretion to investigate potential breaches of law committed by the financial entities within its oversight. If a matter falls within ASIC's regulatory responsibility, it will be assessed to determine whether a formal investigation should be held. This includes consideration of the harm suffered by consumers, potential benefits of pursuing the misconduct in contrast with the expense, level of misconduct available on the evidence and any alternative courses of action, such as surveillance.

While primarily responsible for regulating Australia's corporate, market and financial sectors, the nature of the modern global economy requires ASIC to work internationally with foreign agencies, as many Australian financial market participants undertake cross-border transactions and operations.

ASIC and other international regulators cooperate by sharing information to assist each other with the supervision of markets and enforcement of regulation. This is done in accordance with MOUs ASIC has with other regulators (including multilateral MOUs) and staff secondments with fellow members of the International Organization of Securities Commissions (IOSCO).

ASIC is actively engaged with international partners – including international organisations, foreign regulators and law enforcement agencies – in fulfilling its mandate. This involves cooperation in investigations, compliance and surveillance as well as more generalised interaction on policy research and delegations.

Furthermore, ASIC participates in various international regulatory forums, including IOSCO, and is a signatory to international cooperation agreements, including multilateral and bilateral MOUs.

Many international organisations and foreign regulators make requests for assistance under international cooperation agreements, including MOUs. In some instances, ASIC uses the Mutual Assistance in Business Regulation Act

1992 (Cth), which empowers ASIC to compulsorily obtain documents, information or testimonies on behalf of foreign regulators.

The multilateral MOUs to which ASIC is a signatory include the IOSCO Multilateral Memorandum of Understanding (MMOU), the IOSCO Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information, and the IOSCO Administrative Arrangement.

Established in 2002, the MMOU sets out how signatory regulators from around the world should consult, cooperate and exchange information for the purpose of regulatory enforcement regarding securities markets. Under the MMOU, information requests can be made when regulatory authorities are in the process of investigating offences relating to activities under the relevant laws and regulations of the jurisdictions in question, including the following:

- insider dealing and market manipulation;
- misrepresentation of material information and other fraudulent or manipulative practices relating to securities and derivatives;
- the solicitation and handling of investor funds; and
- the registration, issuance, offer or sale of securities and derivatives.

ASIC's 'why not litigate' approach – developed in the aftermath of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (the final report of which was submitted in 2019) – has continued to result in a proactive approach to the initiation of court proceedings, including in respect of investigations with international elements such as foreign exchange providers and the provision of travel insurance. Some examples are as follows:

- In December 2020, ASIC launched Federal Court litigation, seeking civil penalties, against Union Standard International Group and its former authorised corporate representatives regarding the provision of foreign exchange products to persons in China, in circumstances where those persons were placed at risk of contravening Chinese domestic law. ASIC's allegations include that the company failed to provide financial services efficiently, honestly and fairly.
- In June 2022, Allianz Australia Insurance Limited and AWP Australia Pty Ltd pleaded guilty to a total of seven criminal charges brought by ASIC for allegedly making false or misleading statements in relation to the sale of domestic and international travel insurance. The civil action against the companies resulted in an order from the Federal Court for the companies to pay AU$1.5 million in penalties.

- In March 2021, ASIC banned five persons associated with Forex Capital Trading Pty Ltd, a foreign exchange provider, from providing financial services (for varying lengths of time) on the basis of numerous breaches of the Corporations Act. Separately, in June 2021, the Federal Court ordered the company to pay an AU$20 million civil penalty for breaches of the Corporations Act.

The Australian Competition and Consumer Commission

The Australian Competition and Consumer Commission (ACCC) is an independent commonwealth statutory authority whose principal role is to enforce the Competition and Consumer Act 2010 (Cth) (C&C Act). Most of the ACCC's enforcement work is conducted under the provisions of the C&C Act, although its role also encompasses other legislation.

Similar to many regulators, the ACCC uses a range of compliance tools to prevent breaches of the Act, including business and consumer education, and working closely with stakeholders and other agencies. However, the Act also provides the ACCC with a range of enforcement remedies, including court-based outcomes and court-enforceable undertakings.

In addition to this, the ACCC has increasing international capabilities to assist it with its investigations, including MOUs and treaties with multiple countries for the exchange of information in cross-border investigations, particularly with respect to cartel conduct as well as consumer scams and frauds. In addition to treaties and MOUs of specific relevance to its mandate, the ACCC's work is also engaged by the portions of Australia's free trade agreements that relate to competition law. The ACCC has articulated the aims of its international activities in the following terms:

> *Effective enforcement of Australia's competition, consumer protection and product safety laws in a global economy requires cooperation with similar agencies across the world.*
>
> *We work closely with our global counterparts on international cartel, merger, competition enforcement, consumer protection and product safety matters that affect Australian consumers.*
>
> *We also work with regulators in other jurisdictions to enhance our approach to economic regulation in Australia.*

The ACCC is accordingly a participant in the International Competition Network (and is currently co-chair of the ICN Framework on Competition Agency Procedures), the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), the ASEAN-Australia and New Zealand Free Trade Area, the Seoul Competition Forum, the East Asia Top Level Officials' Meeting on Competition Policy and the International Consumer Protection and Enforcement Network (ICPEN), which is an informal network of government consumer protection authorities established to encourage international cooperation and the sharing of information about cross-border commercial activities that may affect consumer interests.

The ACCC also has extensive powers to investigate international cartels and may:

- compel the provision of information about a suspected breach of competition law, including providing documents or giving verbal evidence;
- seek search warrants from a magistrate and execute these on company offices and the premises of company officers; or
- notify the AFP, which has other criminal investigative and surveillance powers at its disposal.

On 15 August 2014, the ACCC and the Commonwealth Director of Public Prosecutions (CDPP) signed an MOU regarding serious cartel conduct. The ACCC is responsible for investigating cartel conduct, managing the immunity process and referral of serious cartel conduct to the CDPP for consideration for prosecution. The CDPP is responsible for prosecuting offences against commonwealth law, including serious cartel offences, in accordance with the Prosecution Policy of the Commonwealth.

The past year has seen a continuation of the ACCC and CDPP's appetite for pursuing prosecutions of cartel conduct and other breaches of the C&C Act, which often include international aspects. For example, in June 2022 Vina Money Transfer Pty Ltd, a money remittance business operating in NSW and Victoria, was fined the sum of AU$1 million for giving effect to a cartel provision contrary to s44ZZRG(1) the C&C Act, with four individual offenders receiving prison sentences.

In February 2021, Norwegian shipping company Wallenius Wilhemsen Ocean AS was convicted and sentenced to a AU$24 million fine in relation to cartel conduct. Additionally, in April 2021, the Full Federal Court dismissed an appeal by Volkswagen Aktiengesellschaft against a AU$125 million civil penalty for engaging in deceptive conduct relating to the exhaust emissions of certain Volkswagen-branded motor vehicles that were imported into Australia, contrary to the C&C Act.

The Department of Home Affairs

Established in 2017, the Department of Home Affairs (the Department)'s primary function is to provide coordinated strategic and policy leadership for Australia's national security policy and operations. This includes coordinating Australia's counterterrorism policies with overseas agencies and coordinating with overseas agencies in relation to potential cybercrime and cyberthreats. The Department also has a portfolio that focuses on immigration and migration policies, including border security, entry, stay and departure arrangements for non-citizens, and customs and border control (apart from quarantine and inspection). The Department incorporates the former Department of Immigration and Border Protection and its responsibilities also include the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police, the Australian Border Force, the Australian Criminal Intelligence Commission and AUSTRAC.

The Australian Taxation Office

The Australian Taxation Office (ATO) is a government statutory agency and the principal revenue collection body for the Australian government. The ATO is responsible for administering the Australian federal taxation system, superannuation legislation and other associated matters. It conducts its own investigations and also works closely with partner agencies both domestically and abroad. When the ATO decides to bring criminal charges, it is generally the CDPP that conducts the prosecution.

According to the ATO, revenue collection agencies around the world are increasingly sharing intelligence and expertise in financial investigations to combat tax evasion and organised tax crime. Australia has a network of more than 100 information-sharing agreements with revenue collection agencies from other countries. The ATO has stated that these agreements enabled it to raise assessments valued around AU$549 million in the 2017–2018 financial year.

To address issues presented by income and activities concealed offshore as well as difficulties associated with obtaining information on these matters, the ATO states that it works with governments and organisations around the world to fight tax evasion and crime globally. The ATO's reported cooperative strategies for fighting international tax crime include: participating in information sharing, intelligence gathering, analytics, investigations and audits with international tax administrations, using Australia's bilateral tax treaties and the multilateral convention on mutual administrative assistance in tax matters; working with domestic partner agencies through the Serious Financial Crime Taskforce; entering into information exchange agreements and obtaining information from countries previously regarded as secrecy jurisdictions; and working with the international Joint Chiefs of Global Tax Enforcement (J5) in relation to

information and intelligence gathering and sharing as well as conducting joint operations targeted at criminal activity.

Additionally, the ATO collaborates with international revenue agencies bilaterally, and through groups and forums. For example:

- The OECD, a network that includes more than 30 governments from across the globe, has various taskforces in which the ATO participates, including the Joint Taskforce on Sharing Intelligence and Collaboration (JITSIC) and the Taskforce on Tax Crimes and Other Crimes:
    - the JTSIC is a platform involving 42 national tax administration agencies that seeks to provide its membership with an avenue to collaborate through information sharing and intelligence within the legal framework of effective bilateral and multilateral conventions and tax information exchange agreements; and
    - the Taskforce on Tax Crimes and Other Crimes focuses on the identification, auditing, investigation and disruption of tax and other serious criminal crime typologies, including money laundering and bribery.

- The Global Forum on Transparency and Exchange of Information for Tax Purposes' original focus was to address the use of banking secrecy jurisdictions. The forum, which with 162 members is the largest tax group in the world, is principally directed at information exchange and the development of transparency standards around the world in relation to tax.

The ATO exchanges information with its international treaty partners to ensure correct reporting of income earned overseas by Australian residents as well as income earned in Australia by foreign residents and also works with governments and organisations around the world to fight tax evasion on a global scale. Australia has a network of international treaties and information exchange agreements with over 100 jurisdictions. These include income tax treaties, tax information exchange agreements, estate gift tax treaties, agreements concerning East Timor (relating to resources), the Convention on Mutual Assistance in Tax Matters, the US Foreign Account Tax Compliance Act Intergovernmental Agreement with the United States and various other multilateral tax agreements.

Further examples of inter-agency collaboration in the APAC region

The above Australian law enforcement, investigative and prosecution agencies collaborate under formal partnerships and specialised taskforces as well as on an informal basis.

Similarly, these agencies operate collaboratively with APAC partners to investigate and prosecute transnational crime adverse to Australia's national interests.

A number of these partnerships and taskforces are detailed below.

CDPP Organised Crime and Counter-Terrorism Practice Group

The Organised Crime and Counter-Terrorism Practice Group (Practice Group) of the CDPP is responsible for Commonwealth prosecutions of terrorism, national security, and significant organised crime offending. Such criminal typologies often involve prosecutions that are comparatively complex and resource-intensive. The CDPP has reported that '[t]he work of the [Practice Group] is increasingly of an international nature, reflecting the globalisation of more serious criminal activity'.Cases referred to the Practice Group involve activity that often takes place wholly or partly outside the geographical boundaries of Australia, requiring international cooperation (assisted by the Commonwealth Attorney-General's Department) to secure foreign evidence to enable prosecution of international organised crime and terrorism.

The Practice Group works with numerous partner agencies to exchange evidence to facilitate prosecutions. There is a focus on electronic evidence, which is easier to manage, enabling more efficient searching and collating of relevant evidence.

Key domestic partner agencies include the following:

- the AFP;
- the ASIO;
- the Australian Border Force;
- the ACIC; and
- state and territory police.

International agencies involved in recent engagements include the FBI, the United States Department of Justice, the United Nations Office on Drugs and Crime, United Nations Counter-Terrorism Committee, as well as South Asian judges, prosecutors and police officers.

The Serious Financial Crime Taskforce

Created in 2015 and led by the ATO, the Serious Financial Crime Taskforce (SFCT) is a domestic multi-agency taskforce specifically formulated to combine the investigative powers, operational intelligence and capabilities of Australia's largest law enforcement bodies in targeting complex financial crime.

The SFCT targets activities that occur both within Australia and in foreign jurisdictions. It works closely with international partner agencies, both law enforcement and regulators, governments and organisations across the globe, including countries that are subject to Australia's bilateral tax treaties and tax exchange agreements. The current operational focus of the task force is: cybercrime affecting tax and superannuation; offshore tax evasion; illegal phoenix activity; and serious financial crime relating to the Australian government's Coronavirus Economic Response Package.

The SFCT includes the following agencies:

- the AFP;
- the ATO;
- the ACIC;
- the Attorney-General's Department;
- AUSTRAC;
- ASIC;
- CDPP; and
- the Australian Border Force.

Pacific Transnational Crime Network

The Pacific Transnational Crime Network (PTCN) represents a regional international police services-led criminal intelligence and investigation capability. Developed in 2002 to combat transnational crime in the Pacific, the PTCN consists of over two-dozen domestic and foreign law enforcement bodies from nations in the region, particularly Pacific Island countries.

Prominent members include the following:

- Australia (AFP);
- New Zealand (New Zealand Police);
- Fiji (Fiji Police Force);
- Samoa (Samoa Police Service);
- Tonga (Tonga Police); and

- Solomon Islands (Royal Solomon Islands Police Force).

The express purpose of the PTCN is to build policing leadership in the Pacific region and collectively navigate regional policing challenges through discovery, knowledge, influence and partnerships.

The United Nations Office on Drugs and Crime for Southeast Asia and the Pacific

The United Nations Office on Drugs and Crime (UNODC) operates a regional programme in Southeast Asia that provides strategic oversight for member states to combat transnational organised crime and illicit trafficking in the region. UNDOC describes the focus of the regional programme to be:

- giving clear focus to supporting member states and regional partners in achieving priority crime and drug outcomes in the region; and
- increasing the responsiveness, efficiency and effectiveness of UNODC's support to the region.

The UNODC South East Asia regional programme is constituted to address: transnational organised crime and illicit trafficking; corruption; terrorism threats; criminal justice; and drug and health, and alternative development in the region.

The Mutual Assistance in Criminal Matters Act

In addition to informal agreements and MOUs between Australian government agencies and their international counterparts, the Australian government can also rely on the Mutual Assistance in Criminal Matters Act 1987 (Cth) (the Mutual Assistance Act), which provides formal mechanisms for the provision and receipt of international assistance in criminal matters. Bilateral treaties governing the means by which mutual assistance can be provided are legislated by way of Regulations under the Mutual Assistance Act.

The Mutual Assistance Act provides an express channel through which foreign law enforcement agencies may request the assistance of the Australian government and Australian law enforcement agencies with respect to the conduct of criminal investigations. Bilateral treaties are presently in place governing mutual assistance between Australia and the following APAC jurisdictions: China, Hong Kong, India, Indonesia, South Korea, Malaysia, the

Philippines, Thailand and Vietnam. Various multilateral treaties also form the basis of Regulations to the Mutual Assistance Act, including on the topics of cybercrime, money laundering, corruption and transnational organised crime.

Australian investigative, prosecution and law enforcement bodies collaborate with APAC partners both formally and informally in relation to transnational investigations. Requests for assistance include the exercise of powers of search and seizure and the taking of evidence in the form of oral evidence or written statements. All assistance provided must be in accordance with domestic laws, and state parties to mutual assistance treaties have the ability to refuse requests for assistance.

As disclosed in the CDPP's Annual Report for 2019–2020, the CDPP was responsible for drafting 52 separate assistance requests to 22 separate foreign governments over the 2019–2020 reporting period.

The Mutual Assistance framework does not represent an exhaustive regime for inter-government requests for assistance and cooperation. To this end, the Mutual Assistance Act does not 'cover the field' by which the Australian government can assist a foreign government and the law enforcement agencies in criminal investigations.

Countries that are not signatories to mutual assistance treaties may also request assistance that is assessed on a case-by-case basis by the receiving government or law enforcement agency.

Australia and a number of separate APAC governments are also ratified members to multilateral conventions, including the following:

- the 1965 Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters;
- the 1970 Convention on the Taking of Evidence Abroad in Civil or Commercial Matters;
- the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; and
- the United Nations Convention against Transnational Organised Crime.

The Extradition Act

The Extradition Act 1988 (Cth) (Extradition Act) provides Australia's legislative basis for extradition. Extradition involves a person in a foreign jurisdiction being lawfully transferred to the jurisdiction of a requesting state to serve a sentence or face criminal prosecution. The Extradition Act stipulates the criteria and standards that must be met before the Australian government can make or

accept a request for extradition. It sets out a number of mandatory requirements that must be met before Australia can make or accept an extradition request.

Comparable to the mutual assistance regime, the Extradition Act is the legislative basis under which numerous bilateral treaties are enacted into Australian domestic law.

Australia has bilateral extradition relationships with the following APAC jurisdictions: Cambodia, Fiji, Hong Kong, India, Indonesia, Japan, Kiribati, South Korea, Malaysia, Nauru, Papua New Guinea, Samoa, the Solomon Islands, the United States and Vietnam, as well as others coming under the London Scheme for Commonwealth Countries. As with mutual legal assistance law, Australia is also party to numerous multilateral conventions that provide a legal basis for extradition.

As disclosed in the CDPP's Annual Report for 2019–2020, four people were surrendered to Australia during the 2019–2020 period and a further 13 extradition requests remain outstanding.

Conclusion

Law enforcement and regulatory investigations in Australia are becoming more complex and internationalised in response to ever-increasing globalisation. Australian government agencies and regulators have sought to respond by forming formal and informal collaborations with their international counterparts to enable them to conduct investigations across the globe, as well as putting a greater amount of domestic resources towards international investigations.

* *The authors would like to acknowledge the assistance of solicitors Diana Shahinyan and Liam MacAndrews in updating this chapter*

Dennis Miralis
Nyman Gibson Miralis

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters in the following areas: white-collar and corporate crime; money laundering; serious fraud; cybercrime; international asset forfeiture; international proceeds of crime law; bribery and corruption law; transnational crime law; extradition law; mutual

assistance in criminal law matters; anti-terrorism law; national security law; criminal intelligence law; and encryption law.

He appears in all courts throughout Australia and regularly travels outside of Australia for complex international and transnational criminal law matters.

Phillip Gibson
Nyman Gibson Miralis

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law.

Phillip manages and advises on the most complex criminal cases. In the areas of traditional crime, Phillip has acted in many serious drug matters and high-profile murder trials.

Phillip has vast experience in transnational cases across multiple jurisdictions often involving: assets forfeiture; money laundering and proceeds of crime; cybercrime; extradition; mutual assistance; white-collar crime; Royal Commissions; bribery and corruption; INTERPOL notices; international and national security law; and ICAC and Crime Commission matters.

Jasmina Ceic
Nyman Gibson Miralis

Jasmina Ceic is an experienced white-collar defence lawyer who advises and represents both national and international clients in complex cross-border investigations, with a specialist focus on large-scale tax fraud investigations, money laundering investigations, cybercrime and extradition.

Nyman Gibson Miralis

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, cybercrime, international asset freezing or forfeiture, extradition and mutual assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the United States, Canada, the United Kingdom, the European Union, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

Level 9
299 Elizabeth Street
Sydney NSW 2000
Australia
Tel: +61 2 9264 8884

www.ngm.com.au

Dennis Miralis
dm@ngm.com.au

Phillip Gibson
pg@ngm.com.au

Jasmina Ceic
jc@ngm.com.au

China-related Cross-border Investigation under New Data Protection Legislations

Gao Jun (Gary Gao)

Zhong Lun Law Firm

In summary

This chapter discusses compliance suggestions for multinational corporations and Chinese companies, whether state-owned or private, under new Chinese data protection legislation when dealing in cross-border investigations.

Discussion points

- Potential compliance challenges involved in cross-border investigations
- Limitations on data transfer in the context of cross-border investigations
- Collision between cross-border investigation and Chinese data transfer protection law
- Potential risks during the data collection stage of cross-border investigations
- Compliance suggestions for companies dealing with cross-border investigations
- Suggested regulations to be imposed on data transfers by government
- Suggestions on the collision between Chinese data transfer regulations and data transfer requests by foreign law enforcement agencies

Referenced in this article

- The Data Security Law
- The Personal Information Protection Law
- The Criminal Judicial Assistance Law
- The Securities Law
- The International Criminal Judicial Assistance Law
- Measures for Security Assessment of Cross-border Data Transfer
- Information Security Technology: Guideline for Identification of Important Data (Draft for Comments)
- Regulation on the Standard Contract for the Cross-border Transfer of Personal Information (Draft for Comments)
- Guidelines for the Declaration of Security Assessment for Cross-Border Data Transfer

Since the second half of 2021, China has witnessed a rapid evolution of its data protection regime, with strict controls and regulations being imposed on cross-border data flows and personal information protection. Namely, two Chinese data protection legislations have taken effect: the Data Security Law (DSL) on 1 September 2021, and the Personal Information Protection Law (PIPL) on 1 November 2021. Subsequently, supportive implementing regulations and guidance have been released, such as the Measures for Security Assessment of Cross-border Data Transfer (Cross-border Data Transfer Security Assessment Measures),[1] Regulations for the Administration of Network Data Security (Draft for Comments) (Network Data Security Regulations), Information Security Technology: Guideline for Identification of Important Data (Draft for Comments) (Important Data Guideline) and the Regulation on the Standard Contract for the Cross-border Transfer of Personal Information (Draft for Comment) (Regulation on the Personal Information Standard Contract).

Generally, some provisions of the above-mentioned laws are read as 'blocking statutes', particularly in response to the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which gives US enforcement agencies the authority to request companies under their jurisdiction to provide requested data regardless of the territory that the data is stored in. Presumably, these blocking statutes offer companies ways to bypass data requests by foreign law enforcement agencies; however, a few months after the DSL and the PIPL came into effect, in several cases, the judges of US courts opined rejection on the application of the DSL and PIPL in discovery disputes among litigants, barring the production of documents in civil cases. Until now, the question of whether the DSL or PIPL could prohibit the production of documents in criminal proceedings has not been addressed.

Under such circumstances, it could be seen that multinational corporations (MNCs), or Chinese companies – either state-owned or private with businesses or entities in foreign jurisdictions (Companies) – might face a difficult situation between the data provision requested in cross-border government investigation and China's new data protection legislation, which has created new and challenging compliance obligations for Companies.

1 The Cross-border Data Transfer Security Assessment Measures was published on 7 July 2022, and took effect on 1 September 2022.

Potential compliance challenges involved in cross-border investigations

Different layers of limitations set for data transfers in the context of cross-border investigations

Before the DSL and the PIPL came into effect in 2021, provisions in laws and regulations, including the Civil Procedure Law of the People's Republic of China (the Civil Procedure Law), the Securities Law of the People's Republic of China (the Securities Law) and the International Criminal Judicial Assistance Law of the People's Republic of China (ICJAL), were aimed at protecting Chinese entities and individuals from providing evidence and materials to any foreign judicial or law enforcement body without the approval of the Chinese authorities. However, after being supplemented by the newly promulgated CSL and PIPL, there has been a broadening of regulatory boundaries governing cross-border transfers of data, covering stages including the collecting and processing of data, and the recording of information by electronic or other means.

The main relevant provisions of the ICJAL, the Securities Law, the Civil Procedure Law, the DSL and the PIPL are summarised in the table below:

Name of the laws and regulations	Summary of the provisions relating to the cross-border provision of information	No. of the provision	Provision details
ICJAL	The ICJAL restricts entities or individuals in China from providing judicial assistance to foreign prosecutors in support of international criminal proceedings, unless approval from the Chinese government has been obtained in advance.	Article 2	The law applies to criminal judicial proceedings including criminal inquiries, investigations, prosecutions, trials and executions.
		Article 4	Foreign institutions, organisations and individuals shall not conduct criminal proceedings under this law and the institutions, organisations and individuals within the territory of China shall not provide evidence materials and assistance provided for in this law to foreign countries without the approval of the competent Chinese authority.

Name of the laws and regulations	Summary of the provisions relating to the cross-border provision of information	No. of the provision	Provision details
The Securities Law	The Securities Law restricts entities or individuals in China from providing documents or materials to foreign securities regulatory bodies, directly conducting investigations, and evidence collection within the territory of China.	Article 177	Foreign securities regulatory bodies are not allowed to directly conduct investigations and evidence collection within the territory of China. Without the approval of the securities regulatory authorities under the state council and various competent departments of the state council, no entity or individual in China may provide documents or materials related to securities business activities overseas.
The Civil Procedure Law	The Civil Procedure Law restricts foreign bodies or individuals from carrying out the service of documents, and the investigation and collection of evidence, in China without the consent by the relevant Chinese administrative authorities.	Article 284	Request for, and provision of, judicial assistance shall be carried out via the channels stipulated in the international treaty concluded or participated in by China; where there are no treaty relations, requests for and provision of judicial assistance shall be carried out via diplomatic channels. An embassy or consulate of a foreign country based in China may serve documents on a citizen of the foreign country and carry out investigation and collection of evidence but shall not violate the laws of China and shall not adopt mandatory measures. Except for the circumstances stipulated in the preceding paragraph, no foreign agency or individual shall carry out service of documents, investigation and collection of evidence in China without the consent by the relevant administrative authorities of China.
DSL	The DSL forbids entities or individuals in China from providing foreign judicial or law enforcement authorities with data stored within the territory of China without the approval of the competent Chinese authorities.	Article 36	The competent authorities of China shall, in accordance with the relevant laws and the international treaties and agreements concluded or acceded to by China, or on the principle of equality and mutual benefit, handle the requests made by foreign judicial or law enforcement authorities for the provision of data. No organisation or individual within the territory of China may provide foreign judicial or law enforcement authorities with data stored within the territory of the China without the approval of the competent authorities of China.

Name of the laws and regulations	Summary of the provisions relating to the cross-border provision of information	No. of the provision	Provision details
PIPL	The PIPL forbids entities or individuals in China from providing foreign judicial or law enforcement authorities with personal information stored within the territory of China without the approval of the competent authorities of China.	Article 41	The competent authorities of China shall, in accordance with the relevant laws and the international treaties and agreements concluded or acceded to by China or on the principle of equality and mutual benefit, handle the requests made by foreign judicial or law enforcement authorities for the provision of personal information. No organisation or individual within the territory of China may provide foreign judicial or law enforcement authorities with the personal information stored within the territory of the China without the approval of the competent authorities of China.

In this regard, the limitations are generally set as two layers: the first layer would be necessary approvals from the competent authorities following the provisions of ICJAL, the Securities Law and the Civil Procedure Law for the investigations with specific nature, such as the criminal or administrative investigations by foreign agencies (such as the DOJ for violations of the Foreign Corrupt Practices Act (FCPA), US Securities and Exchange Commission (SEC) for violations of federal securities laws or the UK Serious Fraud Office (SFO) for serious or complex fraud, bribery and corruption); and the second would be general approval required by the DSL and PIPL whenever the data falling under their jurisdiction are to be transferred to the foreign judicial or law enforcement authorities. Thus, when encountering any requirements for data transfer in the cross-border investigations, Companies are supposed to review the cases and evaluate the appropriate path that should be followed with regard to what approval should be acquired from which competent Chinese authorities.

In addition, it has been noted that, under DSL and PIPL restrictions, the current common practice – Chinese individual witnesses' or expert witnesses' testimony[2] – normally arises through circuitous approaches, for example, presenting testimony in the location outside the territory of China. Although no penalty or investigation by Chinese authorities has been observed in the public channel, we believe such practice could result in compliance risks.

2 The presentation of witness testimony here referred does not fall under the parameters of the ICJAL, Securities Law or Civil Procedure Law.

The collision between cross-border investigations and Chinese data transfer protection laws

Unlike the GDPR, which allows for more flexibility in interpreting what constitutes a necessary data transfer in the context of cross-border criminal or administrative investigations by explicitly permitting cross-border data transfers under the circumstance that the transfer is either 'necessary for important reasons of public interest' or 'necessary for the establishment, exercise or defense of legal claims', neither the DSL or the PIPL provides such flexibility; on the contrary, they both expressly limit the data and personal information transfer in response to the requirement imposed by the foreign judicial or enforcement authorities by requiring additional approvals from the relevant authorities.

However, as indicated by several decisions recently made by US courts in adjudicating the effect of DSL, PIPL and other blocking statues in discovery dispute, it would not be optimistic for Chinese parties to expect shield from discovery by citing PRC blocking statutes. In *Philips Medical Systems (Cleveland), Inc v Buan and Valsartan, Losartan, & Irbesartan Products Liability Litigation* (D.N.J. 2021), the courts both denied the application of the DSL and likewise reasoned that the DSL only prohibited responsive information from being given to US courts and did not prohibit giving such information to opposing parties. Similarly, in *CF 125 Holding LLC v VS 125 LLC*, the court also rejected the defendant's objection to discovery based on the holding that the DSL failed to be proven to prohibit the production. Further, in the *Valsartan* case, the judge even explicitly expressed that PRC defendants cannot enter the US market expecting a possible shield from unfavourable discovery by PRC blocking statutes. Although these decisions are mainly made against discovery requests and responses traded between parties in civil proceedings, given the congruence of US courts, the trend does not appear optimistic as to whether US courts will grant accommodations to parties citing the blocking statues as an excuse for non-disclosure in investigations.

Potential risks during data collection in cross-border investigations

During an investigation, Companies are generally required to gather data stored in China and provided abroad. Usually, due to the large volumes of data and the various forms by which the data is stored (such as emails and messages), and, most importantly, to earn trust from the authorities initiating the investigation, such as the DOJ, Companies would turn to data collection vendors and attorneys using an authoritative e-discovery platform for the extraction of data from the devices of custodians and the review, analysis, selection, production and submission of electronic evidence or data. Even though the vendors and law firms currently take data protection measures such as using servers based in China and appointing offices based in China to conduct data review and selection to minimise data transfer compliance risks, it is observed that, in light of the perceived tendency towards tightening restrictions regarding data transfers,

many vendors and law firms have been concerned about the risks of being penalised by the Chinese government for direct cross-border submissions of evidence or data to foreign authorities.

Compliance suggestions for companies dealing with a cross-border investigation

Regulations imposed on data transfers by the Chinese government

For the data transfer requirement imposed by the foreign judicial or enforcement authorities, Companies should be alerted about the limitation set by the Civil Procedure Law, ICJAL and Securities Law regarding evidence or material transfer.

With regard to the transfer of data in response to requirements imposed by foreign judicial or enforcement authorities (especially those with criminal enforcement powers or with supervisory powers in relation to their enforcement or judicial activities, such as FCPA enforcement by the DOJ), the ICJAL and the Securities Law provide that any data provision shall be subject to 'government to government' communications and requests such as criminal judicial assistance. The Civil Procedure Law prohibits the collection of evidence by foreign authorities; therefore, in the context of a party responding to a court-issued subpoena or in cases involving government litigants, approvals should be acquired. However, no express prohibition has been imposed on the entities' ability to provide evidence in civil cases to foreign courts on their own initiative. Some examples are given below.

Information transferred as evidence in investigation, litigation or any other activities of a criminal nature by a foreign government or foreign body empowered with criminal judicial authority by a foreign government

Without obtaining prior authorisation by a competent Chinese authority, a domestic Chinese entity may be directed by the DOJ to provide it with information or evidence to assist with an ongoing FCPA investigation, or be ordered to provide evidence in response to a US court order or for the preparation for production of documents in criminal cases. According to the ICJAL, in any such circumstance, the request for criminal judicial assistance should be reported to, and approvals obtained from, competent authorities such as the Judicial Assistance Communication Centre of the Ministry of Justice in advance before providing any such information or evidence. In practice, it would normally take a relatively long period to complete the whole application and obtain the final opinion regarding whether the transfer is permitted.

Documents and materials required to be transferred, in relation to securities business activities overseas and requested by a foreign securities regulatory body

For example, in the absence of an authorisation by the Chinese Securities Regulatory Commission (CSRC), due to the investigation into fraudulent action conducted by the US SEC, a Chinese entity is requested by the SEC to provide it with the documents in relation to listing activities in the US. The documents and materials may not be transferred unless prior approvals have been granted by CSRC.

By contrast, if the request for information or evidence is irrelevant to investigations or proceedings by foreign judicial or enforcement authorities, or if the request is initiated by foreign authorities who possess no administrative powers, the application to a Chinese authority for criminal judicial assistance would not be a necessary step. This would be the case, for example, in circumstances where, without an ongoing FCPA investigation or any other similar foreign enforcement procedure, there are internal investigations into employee misconduct that violates the internal employee handbooks or guidelines initiated by the overseas headquarters of a multinational corporation, and the related facts are in relation to the employees working in China.

Although the motivation for most multinational corporations to conduct an internal investigation is the potential legal leniency under the FCPA where they self-report, conducting internal investigations is a regular self-discipline and self-governance approach for enterprises to effectively supervise and improve themselves. As most headquarters of multinational corporations are located overseas and the governance authority for compliance matters is usually centralised in those headquarters, the cross-border transfer of internal investigation findings gathered in the territory of China could thus be categorised as daily internal governance of an enterprise, rather than preparation for the FCPA investigation that should be subject to criminal judicial assistance.

Similarly, a foreign stock exchange, such as the US NASDAQ Stock Exchange, or derivatives marketplace positioned as a self-regulatory organisation, such as the Chicago Mercantile Exchange (CME), may send inquiries to a Chinese entity, who participates in its market, requesting explanation and supporting documents relating to the financial issue of concern.

NASDAQ, for example, finished its corporatisation and privatisation in around 2017 and is now an independent commercial market player, which has handed over its power of investigating and imposing penalties relating to abnormal trades and dealings to the SEC, and only reserves the power of supervising and monitoring traders and dealers. In view of the nature of NASDAQ's corporatisation, in the case of any abnormal trades or dealings involving financial red flags such as fraud, to improve its efficiency as a competitive stock exchange, it will conduct inquiries into the enterprises concerned and request certain

documents as supporting materials attached to the answers. However, such inquires would not necessarily incur enforcement action by the SEC. According to the express language of Article 177 of the Securities Law, the obligation of the entity transferring data and information to report and obtain approval from the responsible Chinese regulator will be triggered when the domestic entity is requested to provide the relevant materials directly by a foreign securities regulatory body for evidence collection. Thus, the document transfer request imposed by NASDAQ or any other similar stock exchange would normally not trigger the obligation of reporting under the Securities Law. Nevertheless, in practice, there are high risks that unauthorised provision of materials in relation to the securities business activities overseas can be characterised as a violation of article 177 of the Securities Law by regulatory authorities. In this regard, for Chinese entities who receive such request, it would be the usual practice to file the request to the CSRC for the record. Recently, CSRC and SEC have been seeking closer securities cooperation.

Similarly, CME, as a self-regulatory organisation without possessing administrative powers, creates internal committees with responsibility for the investigation, hearing and imposition of penalties for violations of its exchange rules without involving securities regulatory bodies. In light of such nature, it is believed that the data transfer in response to CME's investigation normally requires no approval from the CSRC. However, a close eye should be kept on the updates by CSRC in case any upgrades of its regulatory enforcement.

In international arbitration, a Chinese entity as one party to the arbitration is required to submit evidence to the tribunal located overseas.

Arbitration, unlike litigation before the court, is an alternative method of dispute resolution, chosen by the parties, rather than a typical judicial act conducted by a foreign enforcement authority or authorities with judicial powers. However, in certain circumstance, such as where the witness testimony is ordered by an arbitrator with authority in parallel with a cross-border civil court, there are risks that the cooperative provision of information and evidence without resorting to judicial assistance is a violation of the Civil Procedure Law.

In practice, since arbitration involves less sovereignty, evidence transfer under the arbitration, especially voluntarily provision of evidence by the parties on their own initiative, would not trigger the need for judicial assistance. Nevertheless, as the obligations as to provision of sensitive information and data remains an area of potential liability for the transferrer, such as the deletion or redaction of personal information or important data, this article will elaborate upon the obligations associated with the provision of sensitive information protection in the below.

In addition to the investigation that triggers the obligation set by the Civil Procedure Law, ICJAL and Securities Law, obligations set by article 36 of the DSL and article 42 of the PIPL cover almost every investigation initiated by foreign

agencies with administrative powers, such as export control investigations, sanctions investigations, anti-dumping countervailing duty investigations and customs investigations. Further, during the approval process, attention should be drawn by Companies that many levels of oversight could be involved; for example, a Company engaged in the telecommunications industry may require approval from both the industry-specific department and the national cyberspace authority before engaging in cross-border data transfer. It worth noting that the preparation for performing the obligations set by the multiple layers of regulations, such as submitting the application for approval to both the DOJ and the national cyberspace authority, are recommended to be commenced simultaneously.

After it has been decided that there is no need for approvals or, if needed, the necessary approvals from related competent authorities have been obtained, the next step would be classifying the composition of the requested information and complying with the obligations of cross-border data transfer security assessment. The below table illustrates different obligations triggered by characteristics of data composition.

Laws	Trigger of Obligations	Obligations
Important Data		
Article 31 of the CSL, Article 31 of the DSL	Where providing abroad the important data collected and produced by critical information infrastructure operators	The transfer shall apply for cross-border data transfer security assessment[3] with the state cybersecurity and information department through their local provincial-level cybersecurity and information department.
Article 4 of the Cross-border Data Transfer Security Assessment Measures	Where the data transferred abroad contains important data	

3 According to article 8 of the Cross-border Data Transfer Security Assessment Measures, Cross-border data transfer security assessment focuses on assessing the risks that cross-border data transfer activities may bring to national security, the public interest, and the lawful rights and interests of individuals and organisations, and mainly includes the following matters: (1) the legality, propriety, and necessity of the purpose, scope, method, etc, of cross-border data transfers; (2) the effects on the security of the data transferred abroad of the data security protection policies, laws and regulations, and the cybersecurity environment of the country or region where the foreign receiving party resides; (3) whether the foreign receiving party's data protection level reach the requirements of the laws, administrative regulations, and mandatory national standards of China; (4) the quantity, scope, categories and degree of sensitivity of the data transferred abroad; and the risk of leaks, distortion, loss, destruction, transfer, illegal acquisition, illegal use, etc, during or after cross-border transfer; (5) whether data security and personal information rights and interests are fully and effectively ensured; (6) whether the contract concluded between the data handler and the foreign receiving party fully stipulates data security protection responsibilities and duties; (7) the degree of compliance with Chinese laws, administrative regulations and departmental rules; and (8) other matters that the state cybersecurity and information department determines should be assessed.

Laws	Trigger of Obligations	Obligations
Personal Information		
Article 38 of the PIPL	Where transferring the personal information outside the territory of China due to business or other needs	The transfer shall meet any of the following conditions: 1) pass the security assessment organised by the Cyberspace Administration of China (CAC) in accordance with the provisions of this law; 2) have been certified by a specialised agency for protection of personal information in accordance with the provisions of the CAC; 3) enter into a contract with the overseas recipient under the standard contract formulated by the CAC, specifying the rights and obligations of both parties; and 4) meet other conditions prescribed by laws, administrative regulations or the CAC. According to the Article 4 of the Regulation on the Personal Information Standard Contract, any personal information processor meeting all of the following circumstances may provide personal information abroad by concluding a standard contract: (1) where it is not a critical information infrastructure operator; (2) where it processes not more than 1 million persons' personal information; (3) where it has provided the personal information of not more than 100,000 persons in accumulation overseas since 1 January of the previous year; and (4) where it has provided sensitive personal information of not more than 10,000 persons in accumulation overseas since 1 January of the previous year.

Laws	Trigger of Obligations	Obligations
Personal Information		
		The personal information processor shall inform the individual of such matters as the name of the overseas recipient, contact information, purpose and method of processing, type of personal information and the method and procedure for the individual to exercise his rights against the overseas recipient, and shall obtain the individual's separate consent.
Article 4 of the Cross-border Data Transfer Security Assessment Measures	Where a personal information processor processing the personal information of over 1 million people providing personal information abroad	Additionally, the personal information processor shall apply for cross-border data transfer security assessment with the state cybersecurity and information department through their local provincial-level cybersecurity and information department.
	Where cumulatively providing abroad the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people	
	Where providing abroad the personal information collected and produced by critical information infrastructure operators	

However, given that the Cross-border Data Transfer Security Assessment Measures came into effect on 1 September 2022, the Guidelines for Declaration of Security Assessment for Cross-border Data Transfer was also promulgated on 31 August 2022, the details of submission to security assessment for cross-border data transfer are still waiting to be explored; practically, it is suggested that when facing data transfer request from foreign authorities, Companies could consult Chinese lawyers with experience for further advice in solutions on case-based evaluation, comprehensively considering elements such as the background of the request, the data characteristics, etc.

On the collision between Chinese data transfer regulation and data transfer requests by foreign law enforcement agencies

Considering the long period of Chinese approval-seeking procedures with uncertain results, as well as the compelling force of document production by the foreign law enforcement agencies, concurrent endeavours are still necessary to be undertaken in approaching bilateral competent government authorities to achieve the potential conciliation: data transfer with information necessitated

by Chinese blocking statues. To facilitate such conciliation, the approach with the Chinese authority could be focused on the legality, justice and necessity for the data transfer and specific scope of the data to be caught by the DSL and the PIPL. Concurrently, for the foreign law enforcement agencies, emphasis could be laid around the relationship between the responsive documents and the enforcement of the DSL and the PIPL, and the factors the agencies are concerned with when determining whether a foreign data protection statute can excuse a party from document production (if factors have been established in such jurisdiction). For example, *Aerospatiale-Wultz* factors established by the US Supreme Court included (1) the importance to the case of the information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) availability of alternative means of securing the information; and (5) the relative interests of the United States and the foreign nation.[4]

Nevertheless, there could still be underlying risks in extreme cases. Companies might have no option but to face the either-or choice between a penalty imposed by the Chinese government or a sanction or other adverse result in a foreign jurisdiction.

Gao Jun (Gary Gao)

Zhong Lun Law Firm

Gao Jun is a partner and the head of the compliance and regulatory department of Zhong Lun Law Firm. He has an LLM in the UK and his working languages are English and Chinese. Mr Gao has practised law for 27 years, which makes him an experienced lawyer in both compliance and regulatory as well as international dispute resolution. Before being admitted to the PRC bar in 1995, Mr Gao worked as a criminal judge in a district court in Shanghai for five years.

Mr Gao has been consecutively recommended as a Leading Individual in compliance and regulatory by *The Legal 500 Asia Pacific 2021* and *2020* and in corporate investigation and anti-bribery by *Chambers Asia-Pacific* in years *2018* to *2022*. Mr Gao was also honoured as the 2022 Distinguished Practitioner in Regulatory by Asialaw Profiles; by Benchmark as a Litigation Star in Litigation China and Asia-Pacific in years 2021 and 2022, and as the Litigation Asia-Pacific 2020 Lawyer' for 'the Deal of the Year 2020' by *China Business Law Journal*; a '2020 Band 1 Lawyer of Compliance & Government Affairs', '2019 Band 1 Lawyer of Compliance' and '2019 China Top 10 Lawyers – Government Affairs'

4 See *Société Nationale Industrielle Aérospatiale v U.S. Dist. Court for Southern Dist. of Iowa*, 482 U.S. 522, 96 L.Ed.2d 461 (1987)

by LegalBand; as one of 'The A-List China's Elite 100 Lawyer 2019' by *China Business Law Journal*; the 2017 'Regulatory & Compliance Lawyer of the Year' by *China Law & Practice*; the 2016 'Client Choice Top 20 Lawyer' by *ALB*; and as one of 'Asia's Leading Lawyers for Business of Dispute Resolution' recommended by *Chambers Asia-Pacific 2013*.

Many years of work experience in compliance and regulatory and international dispute resolution has given Mr Gao a comprehensive understanding of international business skills and operations, compliance risks as well as traps that may arise in negotiations. Mr Gao has assisted many multinational enterprises, institutions and large domestic enterprises in different industries in the following matters: compliance issues, including in the context of cross-border investigations, joint investigations by multinational governments and criminal investigations by overseas law enforcement agencies; building comprehensive compliance systems and cybersecurity and data compliance services; in the context of state secrets review, judicial assistance and witness preparation for cross-border investigations; strategies for crisis issues and the design and implementation of firewall programs at home and abroad; criminal law matters, including internal compliance investigations into management; criminal procedures; employee dismissals; and in providing compliance training services to management, employees and business partners.

中倫律師事務所
ZHONG LUN LAW FIRM

Founded in 1993, Zhong Lun Law Firm was one of the first private law partnerships to receive approval from the Ministry of Justice. After years of rapid development and steady growth, today Zhong Lun is one of the largest full-service law firms in China. With over 390 partners and over 2,400 professionals working in 18 offices in Beijing, Shanghai, Shenzhen, Guangzhou, Wuhan, Chengdu, Chongqing, Qingdao, Hangzhou, Nanjing, Haikou, Tokyo, Hong Kong, London, New York, Los Angeles, San Francisco and Almaty, Zhong Lun is capable of providing clients with high-quality legal services in more than 60 countries across a wide range of industries and sectors through our specialised expertise and close teamwork. In recent years, the number of Zhong Lun partners recognised by *Chambers Asia-Pacific* industry guides has surpassed all other Chinese law firms. As a large-scale full-service law firm, Zhong Lun pays special attention to social responsibility and public feedback. By establishing multidimensional and multi-channel rapport with overseas law firms, Zhong Lun has built a diversified and far-reaching global platform to more effectively provide clients with comprehensive and one-stop legal services. Zhong Lun is the only law firm in China that has joined the World Law Group.

6/10/11/16/17F, Two IFC
8 Century Avenue
Pudong New Area
Shanghai 200120
China
Tel: +86 21 6061 3666

www.zhonglun.com

Gao Jun (Gary Gao)
gaojun@zhonglun.com

Singapore: Handling Financial Services Investigations

Joy Tan, Jenny Tsin and Ong Pei Chin

WongPartnership LLP

In summary

Singapore's robust but practical regulatory approach is integral in ensuring that it continues to thrive as a stable, sustainable business and financial hub. In recent years, there has been a shift in our legislative and regulatory framework, from a merits-based approach to a disclosure-based regime. This seeks to encourage a pro-business environment while still allowing for well-managed risk-taking and innovation, underpinned by high standards of financial regulation and strict supervision.

Discussion points

- Singapore's main regulatory bodies for financial regulation and prosecution
- Roles of these regulatory bodies in driving compliance and enforcement
- Tools encouraging voluntary disclosure and self-reporting
- Range of enforcement actions imposed by regulatory bodies
- Considerations for internal investigations
- Singapore's role in international cooperation and enforcement for cross-border investigations

Referenced in this article

- *Pratt Holdings Pty Ltd v Commissioner of Taxation* [2004] 136 FCR 357
- *Regina (Jet2.com Ltd) v Civil Aviation Authority (Law Society Intervening)* [2020] 2 WLR 1215
- Securities and Futures Act (SFA)
- *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v Asia Pacific Breweries (Singapore) Pte Ltd and other appeals* [2007] 2 SLR(R) 367

In just over five decades, Singapore has established itself as the pre-eminent financial centre for the Asia-Pacific region. Home to over 3,000 financial institutions (FIs) across the full spectrum of asset classes, Singapore offers a pro-business environment that allows for well-managed risk-taking and innovation, underpinned by high standards of financial regulation and strict supervision. Particularly in the wake of recent scandals affecting the industry that have had far-reaching consequences, Singapore's robust but practical regulatory approach is integral in ensuring that it continues to thrive as a stable, sustainable business and financial hub.

The main regulatory bodies empowered to undertake financial services investigations and prosecutions are the following:

- The Monetary Authority of Singapore (MAS), which is the central bank and integrated financial regulator of Singapore. It regulates and supervises the financial services sector through administering, among others, the Securities and Futures Act 2001 (SFA), the Financial Advisers Act 2001 (FAA), and the Singapore Code on Take-overs and Mergers. MAS oversees the enforcement of the civil penalty regime for market misconduct. Errant corporates and directors may potentially face civil penalties, Prohibition orders (PO) or licence revocations.[1] On 2 July 2021, MAS issued a consultation paper proposing to strengthen and standardise its investigative powers across various MAS-administered acts, including by requiring a person to appear for examination; entering premises without a warrant; and the transferring of evidence between MAS, the police and the public prosecutor.[2]
- The Singapore Exchange Ltd (SGX), which plays a dual role as both market regulator and commercial entity. SGX manages the day-to-day regulation of listed companies, monitors ongoing compliance with listing requirements and provides support on regulatory issues to listed companies. The regulatory functions of SGX are carried out by an independent regulatory subsidiary, the Singapore Exchange Regulation Pte Ltd (SGX RegCo), which has a separate board of directors to make the segregation of SGX RegCo's regulatory functions more explicit from SGX's commercial and operating activities. SGX RegCo is empowered to investigate infractions of the Listing Rules and to take appropriate disciplinary actions for violations, such as

1 MAS Enforcement Report July 2020 to December 2021 (published April 2022) (the MAS Enforcement Report) at https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/ENF-Report-20202021-PDF.pdf. MAS may also issue reprimands and warnings. One of the noteworthy reprimands to senior management in the past year was of the CEO and director of Aviva Financial Advisers Pte Ltd (Aviva FA) for failure to put in place arrangements to monitor the activities of an external consultant and to address the issue of poor conduct of Aviva FA's representatives (which included misrepresentations to customers regarding the nature and features of certain insurance products).

2 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/2021-FI-Amendment-Bill/Proposed-Amendments-to-MAS-Investigative-and-Other-Powers-under-the-Various-Acts.pdf.

issuing reprimands to non-compliant corporates.[3] SGX RegCo's powers of enforcement were expanded in August 2021 to enable swifter enforcement outcomes.[4]

- The Singapore Police Force (SPF), which has broad investigative powers pursuant to Part IV of the Criminal Procedure Code 2010 (CPC). The Commercial Affairs Department (CAD), which is a specialised division of the Singapore Police Force, investigates a wide spectrum of commercial and financial crimes. Through the Joint Investigations Arrangement, MAS and CAD cooperate to co-investigate all capital markets and financial advisory offences, allowing for the consolidation of investigative resources and further improvement of the effectiveness of market misconduct investigations. In March 2021, the CAD also formed the Anti-Scam Division to 'ensure efficient enforcement coordination and swift information sharing to enhance the scam fighting efforts of the . . . SPF'.[5]
- The Corrupt Practices Investigation Bureau (CPIB), which is an independent agency that reports directly to the Prime Minister's Office. CPIB investigates both public and private sector corruption offences. The powers of investigation of CPIB officers are set out in Part 4 of the Prevention of Corruption Act 1960.
- The Accounting and Corporate Regulatory Authority (ACRA), which regulates business registration, financial reporting, public accountants and corporate service providers. ACRA administers, among others, the Accountants Act 2004 and the Companies Act 1967 and its powers of enforcement are set out in, *inter alia*, section 39 of the Accounting and Corporate Regulatory Authority Act 2004.
- The Competition and Consumer Commission of Singapore (CCCS), which promotes competition in markets by eliminating or controlling practices that potentially hinder competition in Singapore. CCCS enforces the Competition Act 2004 and the Consumer Protection (Fair Trading) Act 2003, taking action against anticompetitive agreements, corporate abuse of dominance in the marketplace and mergers that substantially lessen competition, and protects consumers from such unfair practices.[6]
- The Personal Data Protection Commission (PDPC), which implements policies to promote the protection of personal data and develops Advisory Guidelines to promote compliance with the same.[7]

3 www.sgx.com/regulation/about-sgx-regco#Regulatory%20Functions.

4 https://www.sgx.com/media-centre/20210624-sgx-regco-expands-range-enforcement-powers. See also amendments to the Mainboard Rules and Catalist Rules at https://rulebook.sgx.com/sites/default/files/net_file_store/AMENDMENTS_TO_ENFORCEMENT_(MAINBOARD)_1_August_2021.pdf and https://rulebook.sgx.com/sites/default/files/net_file_store/AMENDMENTS_TO_ENFORCEMENT_(CATALIST)_1_August_2021.pdf respectively.

5 CAD Annual Report 2020 released on 8 October 2021, accessible at https://www.police.gov.sg/media-room/publications?filter=9BC92AE1F3FF452D9CECC3D03C7D5BCB.

6 CCCS' investigation and enforcement powers are set out in Division 5 Part 3 of the Competition Act 2004 and Part 3A of the Consumer Protection (Fair Trading Act) 2003.

7 The PDPC's powers of investigation are set out in Schedule 9 of the Personal Data Protection Act 2012.

Following the completion of investigations, the Attorney-General's Chambers, which has oversight of all prosecutions, may prosecute potential offenders in court.

When handling financial services investigations, it is not only critical to understand the interplay between regulatory agencies, but to address at the outset whether to self-report or cooperate with investigations, and whether legal professional privilege applies.

Self-reporting

Singapore's legislative and regulatory framework is a disclosure-based regime.[8] For offences where a deferred prosecution agreement (DPA) is available,[9] self-reporting may be a factor considered in the prosecution's decisions on whether to enter into a DPA, and on the conditions or any penalty imposed therein.

For companies listed on the Singapore Exchange, Rule 703 of the Listing Manual (LM) requires a listed company to disclose, in a timely manner, any information it has concerning itself, its subsidiaries, or associated companies that is either 'necessary to avoid the establishment of a false market in [its] securities', or that 'would be likely to materially affect the price or value of its securities'. Non-compliance is an offence if intentional or reckless.[10] Directors can also be prosecuted in their personal capacity for the acts of their company, provided the non-compliance was proven to be committed with their 'consent or connivance', or is attributable to their neglect.[11] In addition to the above, listed companies are also obliged to 'comply-or-explain' with regard to deviations from the Code of Corporate Governance (the Code).[12] While variations to the Code are permitted, companies must 'explicitly state and explain' in a comprehensive and meaningful way how their varied practices are 'consistent with the aim and philosophy' of the principles set out in the Code.[13]

Under the CPC and the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA), self-reporting is also required for offences connected with anti-money laundering and counter-financing of terrorism. The CDSA imposes an obligation on individuals to file a suspicious transaction report with CAD as soon as is reasonably practicable once they know or have reasonable grounds to suspect that any property represents the proceeds of, was used in connection with, or is intended to be used in connection

8 Speech by Tharman Shanmugaratnam at the OECD Asian Corporate Governance Roundtable (27 June 2007), www.mas.gov.sg/news/speeches/2007/speech-by-mr-tharman-and-second-minister-for-finance-at-the-oecd2007.

9 See Sixth Schedule of the CPC, these offences include corruption, money laundering, and certain types of market misconduct under the SFA.

10 Section 203 of the SFA; while negligent non-disclosure is not a criminal offence under section 203(3) of the SFA, civil liability can still arise.

11 Section 331 of the SFA.

12 Code at [2] of the Introduction.

13 Code at [8] of the Introduction.

with any act that may constitute criminal conduct, and the information on which the knowledge (or suspicion) is based came to their attention during the course of their trade, profession, business or employment.[14] Individuals who disclose possible offences are given statutory protection, such as immunity against certain civil proceedings and anonymity.[15] Failure to self-report attracts criminal penalties.[16]

Further, FIs and payment services providers are required to self-report under mandatory notices issued by MAS.[17] For example, FIs are required to report any misconduct committed by its representatives, including criminal conduct, inappropriate advice or inadequate disclosure of information to clients, failures to satisfy fit and proper criteria, non-compliance with regulatory requirements, and serious breaches of internal policy or codes of conduct.[18] FIs are also required to undertake internal investigations into their representatives' conduct. Where there has been no instance of reportable misconduct in the course of the financial year, FIs are required to submit an annual nil return.[19]

On 14 May 2021, MAS issued its Response to Feedback from Public Consultation on Revisions to Misconduct Reporting Requirements and Proposals to Mandate Reference Checks for Representatives (the Response)[20] and a Consultation Paper on Proposals to Mandate Reference Checks.[21] In the Response, MAS provided guiding principles to assist FIs in assessing and determining whether a representative has committed an act of misconduct within the reportable categories, and proposed extending the reporting obligation from 14 calendar days to 21 calendar days to allow FIs to establish with reasonable certainty whether a representative has committed misconduct before reporting it to MAS. FIs will also be required to provide to the relevant representative a copy of any misconduct report (and update report) filed, and to take reasonable steps to do so with former representatives. Representatives will in turn be required to provide their current or recruiting FIs with any misconduct report that has

14 Section 45(1) of the CDSA, where a person knows or has reasonable grounds to suspect that any property was used in connection with, represents the proceeds of or is intended to be used in connection with any act that may constitute drug dealing or criminal conduct, and the information on which the knowledge or suspicion is based came to their attention during the course of their trade, profession, business or employment.
15 Sections 45(6), 46 and 47 of the CDSA.
16 Section 45(3) of the CDSA.
17 These notices are issued by MAS pursuant to, *inter alia*, section 101 of the SFA, section 67 of the FAA and section 102 of the Payment Services Act 2019 (PSA). Contravention is a criminal offence under section 101(3) of the SFA, section 67(5) of the FAA and section 102(5) of the PSA.
18 MAS Notice SFA04-N11, Reporting of Misconduct of Representatives by Holders of Capital Markets Service Licence and Exempt Financial Institutions; MAS Notice FAA-N14, Reporting of Misconduct of Representatives by Financial Advisers (Notice FAA-N14).
19 Notice FAA-N14.
20 www.mas.gov.sg/publications/consultations/2018/consultation-paper-on-revisions-to-misconduct-reporting-requirements-and-proposals-to-mandate-reference-checks-for-representatives.
21 www.mas.gov.sg/publications/consultations/2021/consultation-paper-on-proposals-to-mandate-reference-checks.

been filed against them.[22] The Consultation Paper expanded on MAS's proposal to implement mandatory reference checks for FI representatives, extending the ambit of such checks to other significant employees (ie, employees whose misconduct has the potential to detrimentally affect an FI's prudential soundness, reputation, customers' interests or the public's confidence and trust in the financial industry).

In the realm of competition law, CCCS has a leniency programme that offers different levels of benefits to businesses, depending on whether they are the first to come forward with information about cartel activity or on whether investigations have already commenced when they come forward.[23]

CCCS also operates a 'leniency plus' programme, which incentivises businesses that cooperate with CCCS in cartel investigations in one market to inform of their participation in a separate cartel in another market. In this case, applicable businesses may be granted leniency in respect of the second market, and also receive a reduction in the financial penalties in the first market.[24]

Internal investigations

In cases involving certain types of misconduct by their representatives, MAS requires FIs to conduct an internal investigation and keep proper records of, among other things, interviews with relevant parties, documentary evidence of the alleged misconduct, and the investigator's assessment and recommendation.[25] Other scenarios in which FIs may be prompted to launch an internal investigation include the receipt of a complaint from employees or customers, concerns raised by independent directors or their audit committee, incidents of employee misconduct, suspicious transactions, fraud or technology breaches and those in connection with the self-reporting requirements referenced above. Generally, from an FI's perspective, it is important to keep in mind the applicable legal disclosure obligations during the course of the investigations (eg, under the LM or to its directors and shareholders) as well as its reporting obligations under law (eg, under the CPC or the CDSA).

Typical internal investigations involve conducting interviews with relevant employees, management and directors, collection and forensic review of documents, emails, telephone records and electronic device transmissions,

22 Following on from the Response, on 19 April 2022, MAS issued a Consultation Paper on Revised Notices on Misconduct Reporting Requirements under the SFA, FAA and the Insurance Act 1966, inviting responses to the proposed amendments to the relevant Notices, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-on-Revised-Notices-on-Misconduct-Reporting-Requirements.pdf.

23 CCCS Guidelines on Lenient Treatment for Undertakings Coming Forward with Information on Cartel Activity 2016 (effective 1 December 2016) (CCCS Guidelines on Cartel Activity 2016).

24 CCCS Guidelines on Cartel Activity 2016 at [6.1]–[6.3].

25 Notice SFA04-N11; Notice FAA-N14.

and tracing of the proceeds of fraud. External third parties, such as lawyers, accountants, forensic investigators and computer experts, are often asked to assist in the investigations. All individuals being interviewed or investigated may retain their own lawyers, depending on the nature and gravity of the investigations. If there are reasonable grounds to suspect that the investigations may lead to prosecutions or civil action, it is advisable to consider retaining lawyers at an earlier stage so that the statements given during the internal investigations may be considered with the benefit of legal advice.

Care must be taken that there is no breach of banking secrecy under section 47 of the Banking Act (Cap 19) or of personal data under the PDPA in the course of investigations. One way to address the issue is to implement appropriate anonymising of any customer or personal information before it is referenced by the FI concerned.

A key question in internal investigations is the extent to which legal professional privilege can be maintained.[26] In *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v Asia Pacific Breweries (Singapore) Pte Ltd and other appeals* (*Skandinaviska*),[27] the Court of Appeal had to consider whether draft reports submitted by auditors to the company were protected by legal professional privilege. In *Skandinaviska*, Asia Pacific Breweries (Singapore) (APBS) was informed by CAD that its finance manager had fraudulently opened bank accounts in the company's name to borrow money for his personal use, prompting the board of directors to constitute a special committee comprising external auditors and lawyers to investigate and review the company's internal control systems and procedures. Although draft reports were prepared by the external auditors, a final report was never issued.

Legal advice privilege

The Court of Appeal in *Skandinaviska* accepted that communications to and from a third party were not protected by legal advice privilege and that auditors would not be regarded as agents of communication for the purposes of legal advice privilege. The court, however, strongly endorsed the decision of the Australian Federal Court in *Pratt Holdings Pty Ltd v Commissioner of Taxation* (*Pratt Holdings*),[28] which suggested a broader and more flexible approach that was 'principled, logically coherent and yet practical'. In *Pratt Holdings*, communications from third parties were accorded legal advice privilege by focusing on the nature of the function the third party performed, rather than the nature of the third party's legal relationship with the party that engaged it. This has commonly

26 Legal professional privilege covers both legal advice privilege (all confidential communications between a client and his or her lawyer) and litigation privilege (all communications between a client and his or her lawyer and other third parties that were made for the predominant purpose of litigation).
27 [2007] 2 SLR(R) 367.
28 [2004] 136 FCR 357.

been termed as the 'dominant purpose' test. Such an approach accords with modern commercial reality, with parties often engaging the assistance of third-party experts who are not lawyers, and is particularly apposite in cases of large commercial fraud where the victims need expert advice, not only to protect themselves from future fraud, but also to determine the rights and liabilities in connection with the fraud. The Court of Appeal in *Skandinaviska* did not decide on whether the draft auditors' report was subject to legal advice privilege, as this issue was not argued by APBS's counsel. However, if the flexible dominant purpose approach were applied to the facts, legal advice privilege arguably would extend to the legal advice embedded in or that formed an integral part of the draft reports, even though the draft reports were prepared by the third-party auditors and forwarded directly to APBS by those auditors.

The English Court of Appeal in *Regina (Jet2.com Ltd) v Civil Aviation Authority (Law Society Intervening)* (*Jet2*)[29] recently confirmed that the 'dominant purpose' test applied to legal advice privilege, which is in line with the broader and more flexible approach noted in *Pratt Holdings*. While the English position on legal advice privilege appears to be settled following *Jet2*, it remains to be seen whether the 'dominant purpose' test with regard to legal advice privilege would be endorsed by the Singapore courts. That said, given that the Court of Appeal in *Skandinaviska* had strongly endorsed the broader and more flexible approach in *Pratt Holdings*, it is likely that the courts will choose to focus on the nature of the function the third party performed, rather than on the nature of the legal relationship between the parties.

Litigation privilege

The Court of Appeal in *Skandinaviska* found that as the dominant purpose of the draft reports at the time they were created was in aid of litigation, litigation privilege applied to the draft reports. APBS had appointed external auditors and lawyers to determine and quantify the financial impact of the finance manager's fraud and to ascertain APBS's potential liability with regard to the foreign banks. In this regard, as litigation was imminent[30] and 'foremost in the mind' of APBS, such communications were, therefore, protected by litigation privilege.[31]

In light of *Skandinaviska*, it appears that FIs may be able to maintain legal professional privilege over investigation reports, statements and drafts that are created during internal investigations if there is a reasonable prospect of litigation, and legal advice is sought for the main purpose of litigation or

29 [2020] 2 WLR 1215.

30 The Singapore High Court in *Comptroller of Income Tax v ARW and another* [2017] SGHC 16 noted at [37] that where there is a high probability or likelihood of litigation, litigation is likely to be made out to be dominant purpose since a party would be expected to take steps to prepare for the probable and the likely.

31 *Skandinaviska* at [88].

contemplated litigation. The benefit of this is significant: various statutes recognise that powers of investigation that require disclosure of documents and information do not extend to any communications protected by legal professional privilege.[32]

In-house counsel

Legal advice privilege extends to communications with in-house counsel that are made for the dominant purpose of seeking legal advice.[33]

Exceptions to legal professional privilege

These relate to communications made in furtherance of an illegal purpose, or any fact observed by any advocate or solicitor in the course of his or her employment as such showing that any crime or fraud had been committed since the commencement of his or her employment.[34] As for litigation privilege, despite the literal wording of section 131 of the EA, which suggests that litigation privilege is an absolute privilege, in *Gelatissimo Ventures (S) Pte Ltd and others v Singapore Flyer Pte Ltd*,[35] the High Court held that litigation privilege under section 131 of the EA is subject to the same fraud exception found in section 128(2) of the EA.

Procedure for handling privileged material seized

The High Court in *Ravi s/o Madasamy v Attorney General*[36] clarified the procedure for handling legally privileged material seized by the authorities. After considering the approach adopted in the US, Australia, New Zealand and England and Wales, the ourt held that an independent 'privilege team' within the AGC (comprising officers not involved in the underlying investigation) should be the party reviewing the seized materials for privilege. The Court would only determine the matter if there is a dispute. This approach is most similar to the US practice.

32 Section 66(3) of the Competition Act and Sections 30(9)(a) and 34(5) of the CDSA.
33 Section 128A of the Evidence Act (Cap 97) (EA).
34 Section 128(2) of the EA.
35 [2010] 1 SLR 833.
36 [2021] 4 SLR 956

Waiver and limited waivers

The powers to compel disclosure of documents and information to an investigating body do not extend to communications protected by legal professional privilege. In *Yap Sing Yee v Management Corporation Strata Title Plan No. 1267*,[37] the High Court held that statutes will not be regarded to have revoked legal advice privilege unless this is expressly provided for or abrogated by necessary implication.

Such a waiver of privilege in relation to regulators may give rise to the question of whether the waiver may be limited, and whether privilege may still be maintained in other contexts. For instance, in relation to third parties, the UK Court of Appeal has held that a litigant who made clear that waiver was being made only for certain limited purposes was nevertheless able to maintain privilege under circumstances outside those purposes.[38] The Singapore High Court considered this decision in making the ruling that as a particular document had been disclosed only for the purposes of a specific application and that legal privilege had not otherwise been waived, any waiver of legal privilege was limited to the specific purpose of the application.[39] It remains to be seen to what extent Singapore courts will follow this line of reasoning in other contexts, although it would be prudent to seek to expressly limit waiver in any event.

To not inadvertently waive privilege, particularly under circumstances where the reports from internal investigations are required to be submitted to the regulators, mandate letters and strict communication protocols should be implemented at the commencement of any investigation. Should the investigation include a cross-border element, it is critical to establish at the outset the extent to which legal professional privilege may be effective given that not all jurisdictions recognise legal professional privilege, and even for those that do, there are differences in what types of communications are regarded as being privileged. It is also necessary to consider whether the report can be submitted to regulators on a 'limited waiver of privilege' basis, and if so what the scope of this waiver should be. Needless to say, the scope must be carefully and expressly spelt out, so as not to result in waiver that is wider than intended.

Cooperation and DPAs

Generally, FIs and their directors, officers and employees in Singapore are obliged to cooperate with regulatory investigations by the aforementioned authorities. The failure to attend police interviews, produce a document or electronic record, or give information to a public servant when one is legally bound to, or the giving of false statements, are offences under Chapters X and XI of the Penal Code 1871. Further, the failure to appear before MAS and to render

37 [2011] 2 SLR 998.
38 *Berezovsky v Hine & Ors* [2011] EWCA Civ 1089.
39 *Re Vanguard Energy Pte Ltd* [2015] 4 SLR 597 at [57].

all reasonable assistance in connection with investigations, and the failure to produce accounts for inspection, are offences under Part IX of the SFA.

FIs under investigation would be entitled to rely on legal professional privilege and the privilege against self-incrimination. However, in many instances, they may choose to waive privilege and turn over privileged material to regulators, on the basis that full cooperation would be favourably regarded, particularly in instances where regulators may have the discretion to proceed via a civil penalty, via criminal prosecution, or a DPA.

The Criminal Justice Reform Act 2018 (No. 19 of 2018) introduced DPAs into the CPC.[40] Under the DPA framework, companies can seek to avoid criminal prosecution in exchange for compliance with certain conditions,[41] restricted to offences in the Sixth Schedule to the CPC (ie, offences relating to corruption, money laundering, dealing with stolen property or the proceeds of crime, and falsification of records). To become effective, a DPA must be sanctioned by the High Court, which must decide that the DPA is in the interests of justice and that its terms are fair, reasonable and proportionate. The Public Prosecutor can thereafter apply to the High Court to have a 'discharge amounting to an acquittal' granted in favour of the subject company once the DPA has been completed and complied with. Although the viability and usefulness of DPAs has yet to be tested in the Singapore investigations scene, it is clear that the DPA regime is intended to incentivise and encourage a higher level of cooperation with the authorities, which would hopefully assist and lead to a decrease in commission of future offences.

A key condition that may be imposed in a DPA would be to require the company to cooperate in any investigation relating to the alleged offence. In addition, a company may agree to pay a financial penalty, compensate victims of the alleged offence, implement a robust compliance programme, or make changes to an existing compliance programme that will reduce the risk of a recurrence of any conduct prohibited by the DPA.

In terms of the level of cooperation that may be required to enter into an ideal DPA, companies may take guidance from *SFO v Rolls-Royce Plc*. The UK's Serious Fraud Office (SFO) had entered into a DPA with Rolls-Royce and agreed to grant Rolls-Royce amnesty for criminal conduct involving bribery and corruption, in exchange for several terms and conditions (such as a financial penalty and the requirement for Rolls-Royce to cooperate fully and honestly with SFO in relation to any prosecution brought by SFO in respect of the alleged offences). Crucially, SFO observed that its decision to offer the DPA to Rolls-Royce was

40 With effect from 31 October 2018.

41 These conditions include: providing an admission of wrongdoing, paying a financial penalty, disgorging profits, implementing programmes for corporate reform; and assisting in the investigation and prosecution of other wrongdoers. During the second reading of the Criminal Justice Reform Act 2018 in Parliament, the then Senior Minister of State for Finance and Law Ms Indranee Rajah noted that the financial penalties under the DPA regime would not be subject to a statutory maximum.

heavily influenced by the fact that Rolls-Royce had fully cooperated with SFO during its investigations and opened its doors, providing SFO with copies of key documents and access to all relevant emails. Rolls-Royce had also waived legal professional privilege in respect of certain documents or communications, which was viewed as a key indicator of whether a company was genuinely cooperating and deserving of a DPA.

Enforcement and trends

Corporate entities can be subject to both criminal and civil liability for their employees' misconduct. The Interpretation Act 1965 defines a 'person' or 'party' as including 'any company or association or body of persons, corporate or unincorporate',[42] that criminal liability may attach to. A company may also be held liable for its employee's conduct if the latter is considered the 'directing mind and will' of the company.[43] Further, depending on the nature of misconduct involved,[44] companies can be held liable under the SFA for market misconduct committed by employees if the market misconduct was committed with the companies' consent or connivance,[45] or was attributable to the companies' negligence in failing to prevent or detect the employees' market misconduct.[46]

Aside from imprisonment, companies can be subject to most other forms of sanction, including fines, civil penalties or even disqualification from the right to carry out certain actions in the future.[47] Generally speaking, companies face higher financial penalties than individuals, and some offence-creating provisions specifically provide for this.[48] Where the company or offence concerned falls under the purview of a specific regulator (eg, MAS or SGX), additional sanctions may flow from the offence, such as the revocation of or conditions placed upon any licence required.

In recent years, SGX and SGX RegCo have taken a more interventionist approach towards enforcement. As it stands, this trend can be expected to continue, as regulators seek to enhance issuer accountability and investor confidence in the market. SGX's powers of enforcement were expanded in August 2021 to

42 Section 2 of the IA.
43 *Tom-Reck Security Services Pte Ltd v Public Prosecutor* [2001] 1 SLR(R) 327.
44 For example, a company could be liable for insider trading pursuant to sections 218 and 219 of the SFA read with section 226(1) of the SFA, although it has a defence under section 226(2) of the SFA.
45 Section 236B of the SFA; see also MAS: Explanatory Brief on amendments to the SFA 2008, www.mas.gov.sg/news/speeches/2008/explanatory-brief-sfa-amendment-bill-2008-and-faa-amendment-bill-2008 and MAS: Explanatory Brief on amendments to the SFA 2012, www.mas.gov.sg/news/speeches/2012/explanatory-brief.
46 Section 236C of the SFA.
47 For example, where a company has engaged in discriminatory hiring practices, it may be barred by the Ministry of Manpower from applying for new immigration work passes for its employees for a specified period.
48 Namely, those relating to corruption, money laundering, dealing with stolen property or the proceeds of crime, and falsification of records.

enable swifter enforcement outcomes. From 1 August 2021, SGX RegCo has the powers to:

1. issue a public reprimand and require issuers to comply with specified conditions;
2. prohibit issuers from accessing the facilities of the market for a specified period or until the specified conditions are fulfilled;
3. prohibit issuers from appointing or reappointing a director or an executive officer for up to three years; and
4. require a director or an executive officer to resign.

Although SGX RegCo's powers under (1) are non-appealable, the regulator's powers under (2) to (4) are appealable before the Listing Appeals Committee.[49]

From 1 January 2022, issuers will also be required to state in their annual reports that they have an appropriate whistle-blowing policy in place, as well as provide an explanation of how they have complied with certain key requirements such as having independent oversight of the policy and commitment to protecting the identity of whistle-blowers.[50]

On 27 April 2022, MAS released its Enforcement Report for July 2020 to December 2021.[51] The average time taken by MAS to complete reviews and investigations decreased from 24 to nine months in criminal cases, and from 26 to 19 months in civil penalty cases. The key areas of focus were market abuse (such as false trading), financial services misconduct (including mis-selling of financial products) and money laundering-related control breaches. Enforcement outcomes included seven criminal convictions, $2.59 million in financial penalties and compositions, one licence revocation and 20 POs. MAS also introduced a new section providing updates on the status of selected ongoing major investigations, which take longer to complete due to, *inter alia*, their complexity or cross-border elements necessitating assistance from foreign regulators.[52] These updates provide summaries of actions taken, statuses of the investigations and in the case of Noble Group Limited, an indication when the joint investigation hopes to reach a conclusion.[53]

49 http://rulebook.sgx.com/sites/default/files/net_file_store/AMENDMENTS_TO_ENFORCEMENT_(MAINBOARD)_1_August_2021.pdf; https://rulebook.sgx.com/sites/default/files/net_file_store/AMENDMENTS_TO_ENFORCEMENT_(CATALIST)_1_August_2021.pdf.

50 www.sgx.com/media-centre/20210624-sgx-regco-expands-range-enforcement-powers.

51 https://www.mas.gov.sg/news/media-releases/2022/mas-reports-strong-enforcement-outcomes-and-publishes-updates-on-major-investigations.

52 These cases are the investigations into (1) Noble Group Limited; (2) Hyflux Ltd; (3) Eagle Hospitality Trust and (4) Hui Xun Asset Management Pte Ltd (formerly known as Envysion Wealth Management Pte Ltd).

53 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/ENF-Report-20202021-PDF.pdf. Enforcement actions taken by MAS in the past five years are also

In April 2022, Parliament also passed the Financial Services and Markets Bill 2022.[54] The new Financial Services and Markets Act 2022 (FSM Act) will expand and harmonise MAS' powers to issue POs (which currently reside in various industry specific Acts): (1) the categories of persons that may be subject to POs are expanded; (2) Instead of specific acts of misconduct, the ground for issuing POs is a single fit and proper test comprising the elements of (a) honesty, integrity and reputation; (b) competence and capability; and (c) financial soundness. This is consistent with the approach taken in the UK. The FSM Act will also regulate all virtual asset service providers created in Singapore, and which provide services relating to these virtual assets outside Singapore.[55]

Also on the cryptocurrency front, on 30 June 2022, MAS reprimanded the cryptocurrency hedge fund, Three Arrows Capital Pte. Ltd. (Three Arrows), for providing false information to MAS and exceeding the assets under management threshold allowed for a registered fund management company. It is also assessing if there were further breaches of MAS' regulations by Three Arrows.[56] In an interview with the Financial Times, the chief fintech officer at MAS also stated that it will be 'brutal and unrelentingly hard' on bad behaviour in the crypto industry.[57] Greater regulatory scrutiny on cryptocurrency players may be expected moving forward.

International cooperation

Singapore has adopted various international conventions into its domestic law (eg, the CDSA, the Terrorism (Suppression of Financing) Act 2002, the Extradition Act 1968 and the Extradition (Commonwealth Territories) Declaration, the United Nations Act 2001, and the Mutual Assistance in Criminal Matters Act 2000), which facilitate the provision and obtaining of international assistance in criminal matters. These international conventions facilitate the provision and obtaining of evidence, arrangements for parties to give evidence or assist in criminal investigations, and the forfeiture or confiscation of property in the recovery. Singapore is also party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters, which provides a platform for countries in the region to request and give assistance in the collection of evidence for criminal investigations and prosecutions.

published by MAS at https://www.mas.gov.sg/regulation/enforcement/enforcement-actions?page=1&q=reprimand&sort=&rows=10#.

54 https://sso.agc.gov.sg/Acts-Supp/18-2022/Published/20220511?DocDate=20220511.

55 See the Explanatory Brief on the first reading of the bill https://www.mas.gov.sg/news/speeches/2022/explanatory-brief-for-financial-services-and-markets-bill-2022 and the speech on the 2nd reading of the bill. https://www.mas.gov.sg/news/speeches/2022/financial-services-and-markets-bill-second-reading-speech-on-4-april-2022.

56 https://corp.sgx.com/media-centre/20210624-sgx-regco-expands-range-enforcement-powers.

57 *Financial Times*, 'Singapore regulator vows to be "unrelentingly hard" on crypto' (23 June 2022) at https://www.ft.com/content/aae591e1-b291-493c-94c6-6babcb682831.

The regulatory authorities in Singapore also work with other foreign regulatory bodies on such initiatives. For instance, the Singapore Police Force is a member of Interpol while MAS is a signatory to the IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information. In connection with this, MAS is empowered under the SFA to provide assistance to its foreign counterparts in foreign investigative and enforcement actions. Under section 172(1) of the SFA, MAS may, in relation to a request by a foreign regulatory authority for assistance, transmit such information in its possession or order any party to furnish MAS with that information. MAS may also order any person to furnish such information directly to the foreign regulatory authority where there is an ongoing investigation or enforcement by the foreign authority.[58]

Conclusions and outlook

Financial services investigations have not slowed down in the past year notwithstanding the challenges posed by the covid-19 pandemic. The various regulatory authorities also continue to work on enhancing the regulatory framework and enforcement regime, to for greater effectiveness in addressing misconduct in the financial sector. These demonstrate Singapore's commitment to maintaining its position as a trusted financial hub.

Joy Tan

WongPartnership LLP

Joy Tan is the joint head of the commercial and corporate disputes practice, the corporate governance and compliance practice and the financial services regulatory practice.

Her main practice areas are banking, corporate and commercial dispute resolution and contentious investigations. She also regularly advises on corporate governance and financial services regulatory matters under the Companies Act, Securities and Futures Act and other regulatory statutes, including in relation to corporate fraud, anti-money laundering issues and market misconduct. She has represented corporations and shareholders in disputes relating to fraud, minority oppression, corporate transactions and share valuations.

58 Section 172(1)(c) read with section 172(2) of the SFA.

Joy graduated with first class honours from Cambridge University. In 1992, she was awarded the UK Council of Legal Education Prize at the Non-Vocational Bar Exam. Joy is admitted to both the English Bar and the Singapore Bar. She joined the Singapore Legal Service as a Justices' Law Clerk with the Singapore Supreme Court before entering private practice.

Joy is a fellow of the Chartered Institute of Arbitrators, sits on the Panel of Arbitrators of the Singapore International Arbitration Centre (SIAC), and is also a panel member of The Law Society Disciplinary Tribunals appointed by The Honourable Chief Justice under the Legal Profession Act.

Jenny Tsin

WongPartnership LLP

Jenny Tsin is the joint head of the employment practice and a partner in both the commercial and corporate disputes practice and the corporate governance and compliance practice.

Jenny is experienced in all aspects of employment law, with particular focus on preventing and resolving disputes between employers and employees. In addition to employment-related disputes, Jenny's dispute resolution experience extends to shareholder disputes, commercial and contractual disputes and claims relating to directors' duties, auditors' duties and other corporate governance matters and has experience in both litigation and arbitration.

On the investigations front, Jenny frequently handles sensitive and complex investigations relating to employee misconduct and workplace safety issues. Jenny has led investigations relating to sexual harassment, conduct that potentially amounts to breaches of sanctions and other financial regulations, privacy breaches, and landmark cases where workplace safety breaches led to loss of lives.

As a partner in the corporate governance and compliance practice, Jenny advises and speaks on provisions of the Securities and Futures Act, the Companies Act and other regulatory statutes. Jenny has an interest in issues relating to corporate fraud, anti-money laundering and insider trading. Jenny routinely advises and assists corporations in their investigations of such issues.

Ong Pei Chin

WongPartnership LLP

Ong Pei Chin is a partner in the corporate and regulatory investigations and commercial and corporate disputes practices.

Pei Chin regularly advises clients on various governance and compliance issues under the Companies Act, Securities and Futures Act and SGX Listing Rules. She has practical experience reviewing compliance issues from a regulator's perspective from her stint at the Monetary Authority of Singapore. She has also obtained the International Compliance Academy's Advanced Certificate in Governance, Risk and Compliance, accredited under the Institute of Banking & Finance, scoring a distinction on the course.

Pei Chin advises and assists clients on regulatory investigations initiated by various bodies including Singapore Exchange Regulation, the Accounting and Corporate Regulatory Authority and the Competition and Consumer Commission of Singapore, as well as on internal investigations raising bribery and corruption concerns.

Headquartered in Singapore, WongPartnership is an award-winning law firm and one of the largest in the country. As a leading provider of legal services, we offer our clients access to our offices in China and Myanmar, and in Abu Dhabi, Dubai, Indonesia, Malaysia and the Philippines, through the member firms of WPG, a regional law network. Together, WPG offers the expertise of over 400 professionals to meet the needs of our clients throughout the region.

Our expertise spans the full suite of legal services to include both advisory and transactional work where we have been involved in landmark corporate transactions, as well as complex and high-profile litigation and arbitration matters. WongPartnership is also a member of the globally renowned World Law Group, one of the oldest and largest networks of leading law firms.

At WongPartnership, we recognise that our clients want to work with the best. As a partnership of exceptional individuals, we are committed in every way to make that happen.

12 Marina Boulevard, Level 28
Marina Bay Financial Centre, Tower 3
Singapore 018982
Tel: +65 6416 8000
Fax: +65 6532 5711/5722

www.wongpartnership.com

Joy Tan
joy.tan@wongpartnership.com

Jenny Tsin
jenny.tsin@wongpartnership.com

Ong Pei Chin
peichin.ong@wongpartnership.com