

GIR INSIGHT

ASIA-PACIFIC
INVESTIGATIONS REVIEW
2020



ASIA-PACIFIC INVESTIGATIONS REVIEW 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2019
For further information please contact Natalie.Clarke@lbresearch.com

LAW BUSINESS RESEARCH

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL
© 2019 Law Business Research Ltd
www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of August 2019, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – david.samuels@lawbusinessresearch.com

© 2019 Law Business Research Limited

ISBN: 978-1-83862-225-1

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Cross-border overviews

Artificial Intelligence and Machine Learning1

Weng Yee Ng and James Norden

Forensic Risk Alliance

Data Privacy and Transfers in Investigations13

Daniel P Levison, Sheryl J George, David Hambrick and Daniel Steel

Morrison & Foerster LLP

Forensic Accounting in Cross-border Investigations.....30

Colum Bancroft and Edward Boyle

AlixPartners

**The Long Arm of Law Enforcement in
Multi-jurisdictional Investigations41**

Kyle Wombolt, Jeremy Birch and Christine Cuthbert

Herbert Smith Freehills

Country chapters

Australia: An Increasingly Global Approach53

Dennis Miralis and Phillip Gibson

Nyman Gibson Miralis

Australia: Handling Internal Investigations70

Rani John, James Morse and Natalie Caton

DLA Piper

Cambodia: Anti-corruption.....84

David Mol

Tilleke & Gibbins

China: A New Normal Amid Rising Trade Tensions.....93

Dora W Wang, Michael Lowell, Peter Witherington and Jessica Tian

Reed Smith

Contents

Hong Kong: Regulatory Developments in the New Technological Era..... 105
Maria Sit, Irene Lee and Natasha Shum
Dechert

India 118
Aditya Vikram Bhat and Prerak Ved
AZB & Partners

Indonesia 129
Maurice Burke, David Gargaro, Khushaal Ved, Teguh Darmawan and Dyah Paramita
Hogan Lovells

Laos: Anti-Corruption Laws Key to Economic Development 139
Dino Santaniello
Tilleke & Gibbins

Myanmar: Continuing the Fight against Corruption 151
Nwe Oo and Sher Hann Chua
Tilleke & Gibbins

Singapore: Handling Financial Services Investigations 161
Joy Tan and Koh Swee Yen
WongPartnership LLP

Thailand: Anti-corruption Compliance 176
Michael Ramirez
Tilleke & Gibbins

Vietnam: Compliance Risks 184
John Frangos
Tilleke & Gibbins

Preface

Welcome to the *Asia-Pacific Investigations Review 2020*, a *Global Investigations Review* special report. *Global Investigations Review* is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing, telling them all they need to know about everything that matters.

Throughout the year, the *GIR* editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products. In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than our journalistic output is able.

The *Asia-Pacific Investigations Review 2020*, which you are reading, is part of that series. It contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.

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 write to insight@globalinvestigationsreview.com.

Global Investigations Review

London

August 2019

Artificial Intelligence and Machine Learning

Weng Yee Ng and James Norden
Forensic Risk Alliance

Introduction

Artificial intelligence (AI) and machine learning— one may think that these fashionable or sexy buzz words are bandied about to pique the interest of the general public; on the contrary, these are increasingly common terms in the areas of investigation and compliance programmes. Digital technology is so prevalent in our day-to-day lives that most activities leave some form of data footprint. As we embrace technology and the convenience it brings to our daily lives, especially in an increasingly connected world, this contributes to an explosion of data.

As investigators and compliance professionals, we are all well versed on the complexity of the matters that we deal with. Although advancement in technology adds to this increasing complexity around an investigator's modus operandi, technology has also helped investigators navigate large volumes of information across different data sets to find the needle in the haystack.

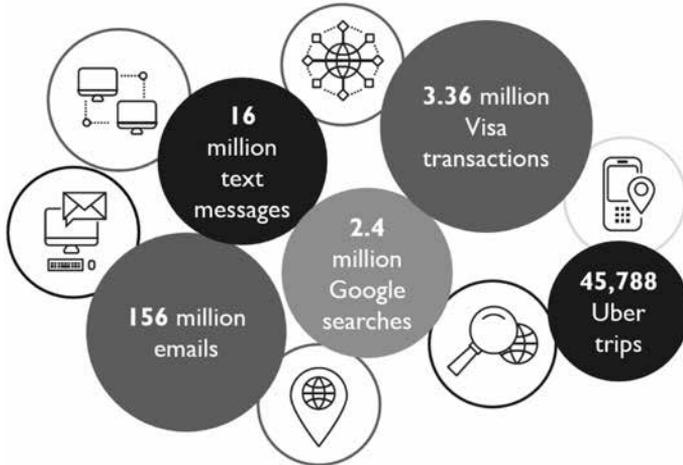
The growing data landscape

In an investigation or in a compliance programme, we are often exposed to a variety of systems and tools where data is held, including back office systems, customer relationship systems, social media, machine-generated data, mobile applications and communications. The data sets could be anything from text posted on social media to accounting entries from structured enterprise resource planning (ERP) systems, where specific data mining processes are deployed for the respective data sets. There is also 'big data' – data sets that are so large in volume and complex in structure that the storing and processing steps applied to smaller data sets would not be adequate or appropriate, and a different process is required.

According to an article published by *Forbes* in 2018, 90 per cent of the world's data was generated over the past two years alone.¹ Business emails are forecasted to exceed a staggering 293 billion per day in 2019 and this number is forecasted to balloon further to over 347 billion

1 <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7786b97460ba>.

by the end of 2023.² This is indicative of the vast volume of data that investigators need to be prepared to manage in an investigation and, in particular, the importance of finding solutions for efficiently wading through all of the information collected to isolate the critical evidence. Often, traditional news media and social media data is used to triangulate information obtained during investigations through other means, including both structured and unstructured data.



Data generated per minute
Source: Forbes (2018)

Harnessing this wealth of data is sometimes challenging due to the volume and the location of the sources available. The number of social media users worldwide as at February 2019 was noted to be approximately 3.4 billion, which reflects a 9 per cent year-on-year increase.³ In typical investigations, results of internet searches are often manually overlaid on the review of unstructured data and analysis of structured data, which can be time-consuming, inefficient and insufficiently robust.

Chat applications such as WhatsApp and WeChat, in-house communication tools and other applications are now a normal part of life and business. Recent years have also seen an increase in ‘fake news’ and innuendo, which distorts information and patterns. The ability to stratify data in order to distinguish innuendo from fact is critical in establishing credible and reliable evidence.

Furthermore, in an era where time is money and information is power, business negotiations and sensitive company information are increasingly being exchanged via these tools. From a payment or funds movement perspective, recent years have seen a shift from traditional

2 <https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210>.

3 <https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>.

payment formats (eg, cash, cheques, credit and debit cards) to alternative payment methods (eg, digital wallets, digital payment applications such as WeChat Pay and cryptocurrencies). These newer methods add to the complexity of the data landscape an investigator needs to navigate.

As ever-increasing amounts of data are created everyday, it is important to understand that data quality is also central to AI development. Large volumes of good quality data are required in order to design the queries and algorithms, perform effective machine learning and test the output.

Demystifying AI and machine learning

Before exploring the application of AI and machine learning in investigations and compliance programmes, we should first define what AI and machine learning truly mean in this context. It is tempting, and somewhat naïve, to think of AI and machine learning as the computer doing all the hard work, where in reality these intuitive technologies are based on algorithms written by AI engineers to follow precise instructions.

Let us start with demystifying AI. AI is built on the basis of learned behaviour, which is developed as a result of experience.⁴ It goes beyond the automation of manual tasks by performing tasks frequently and on a large volume of data, producing reliable results. Progressive or self-learning algorithms and back propagation take AI one level further, to where the system teaches itself to predict the next steps and self-adjust through training and added data.

Machine learning is a subset of AI. Supervised machine learning, for example, requires human input to drive learning, whereas unsupervised machine learning generates insights without human intervention. Machine learning is used to identify and build trends and patterns based on the data processed, which then points to transactions, documents and conversation threads that may be of interest to the investigation team. In machine learning, humans do not encode their expertise directly as the algorithms are designed to autonomously improve their performance. This is also known as 'data-driven AI' and recent advances in this field have been catalysed by the availability of large volumes of data.

One should not go so far as to think that human involvement is not required and that robots are taking over. Human input is essential to design appropriate questions and to evaluate the output generated, in particular, in working out the strategy for dealing with illogical output.

4 <https://www.khanacademy.org/science/biology/behavioral-biology/animal-behavior/a/learned-behaviors>.

Applying AI and machine learning to investigations

Before one balks at the idea that AI and machine learning in investigations are brand new inventions too complicated to deploy, let us put this into the perspective of how we already use some of these technologies.

In document reviews, we use technology to help identify key terms, eliminate noise and false positives, and narrow down the population of documents that may be of relevance to the investigation, thereby saving valuable time. Tools are also used to search for clusters of words that have already been translated by experts and predictive coding is used in technology-assisted review (TAR). The application of AI on images and sound files are more challenging than text as a large volume of data is required to train AI. However, it is not impossible. Facebook, for example, has a facial recognition programme, which is trained through millions of photos that were diligently labelled by its users.⁵

For structured data, we use AI to help us profile the data, identify key patterns and isolate potential red flag transactions. Dashboards, data profiling and visualisation, trend analysis and detection of anomalies are but a few examples of what AI can do with structured data.

AI can also be configured to eliminate non-responsive, privileged, confidential or private materials and those responsive to state secrecy, national security and other jurisdiction-specific requirements. Similarly, sensitive communication can be redacted so that the human reviewer never sets eyes on it, thereby safeguarding highly sensitive and valuable data.

For cross-border investigations, such methods could be configured to perform cross-border deduplication or be combined with other technologies. For example, when combined with hosting data in-jurisdiction or using a mobile in-country solution with air gap, whether on a client site or behind client firewalls, all these technological advancements help maximise the benefit to the investigation team.

In the future, or even today for some, AI will offer the ability to synthesise structured data and integrate findings from the review of unstructured data into the analysis of structured data. The latter is extremely powerful as systems and data sets do not naturally interface with one another and being able to overlay the results of a review into other data analysis introduces increases in efficiency and reductions in errors. Such integration and application in tandem requires close collaboration between lawyers, forensic accountants and data experts, as it is important to ensure that the configuration is set correctly. When designed and deployed appropriately, it can lead to a very effective form of supervised machine learning.

5 <https://www.forbes.com/sites/nicolemartin1/2019/01/17/was-the-facebook-10-year-challenge-a-way-to-mine-data-for-facial-recognition-ai/#cc37c8c58597>.

Applying AI and machine learning in compliance programmes

The application of AI and machine learning is not limited to investigations only. Using readily available data, companies should, if not done already, use AI and machine learning in their continuous compliance monitoring process. This can be especially beneficial to in-house compliance teams that are small with limited resources but are nevertheless tasked with the enormous responsibility of ensuring compliance with various regulations and legal requirements across every jurisdiction.

AI deployed in compliance programmes can bring the following benefits.

Coverage

Larger populations (of operations and entities) can be reviewed as AI allows for processing of large volumes. This means that compliance teams are able to monitor not only central operations (eg, headquarters), but also subsidiaries operating around the world. The lack of oversight of operations in foreign jurisdictions has frequently been noted as one of the weaknesses for companies that have an international presence.

Consistency

Algorithms are built based on defined rules as set out within the company's policies and procedures, which are then applied consistently across all data collected. This removes the inconsistency in testing methodology, which can happen when transactions are reviewed and selected for testing by different individuals, and is easier to defend as the methodology and process are auditable.

Efficiency

The AI process is fast, accurate and requires much less human intervention (except for evaluating the output). With sufficient data and training, self-learning algorithms can be designed, which simultaneously increases the accuracy and reduces processing time.

A second line of defence

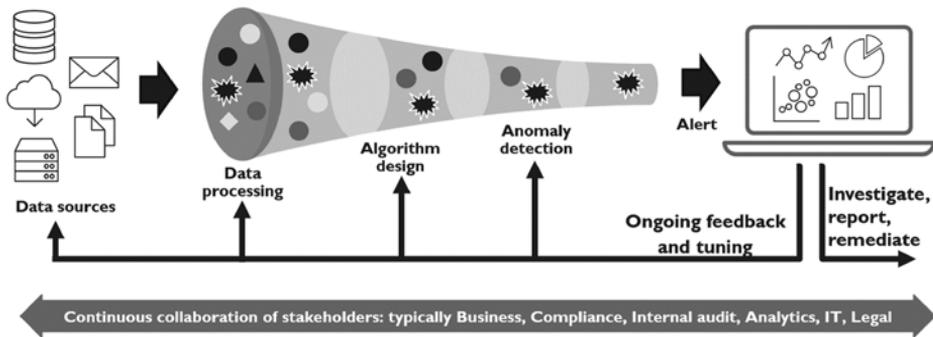
Designed appropriately, AI can be used to support the compliance and risk management teams in establishing a robust second line of defence, in particular through the monitoring of effective implementation of risk management controls.

Real-time detection (which drives remediation)

AI enables real-time detection of potential anomalies that are then escalated to the appropriate channels and appropriate remediation can be deployed shortly thereafter to refine the algorithms and mitigate the risks or weaknesses identified.

Defendable

Most importantly, an AI approach is repeatable and defendable to both internal and external stakeholders.



Usage of AI by governments and regulators

The use of AI and machine learning by regulators is also on the rise, in particular in the area of enforcement and supervision. In particular, there is an ever-increasing expectation for corporates to proactively identify instances of fraud and breaches of laws and regulations, self-report to the relevant authorities and remediate in a timely fashion.

As far back as 2012, in the case *Da Silva Moore v Publicis Group Magistrate*, Judge Andrew Peck of the US District Court in the Southern District of New York approved the use of predictive coding to cut through the large volume of documents to be reviewed.⁶ Fast forward to August 2017, where AI and machine learning have further advanced, the US Department of Justice (DOJ) announced a task force targeting opioid abuse, in which the centrepiece was a data analytics programme monitoring opioid prescriptions nationwide.⁷

In the UK, the *Pyrrho Investments Ltd v MWB Property Ltd* case in 2016 became the first case in the UK where the use of TAR was approved.⁸ Two years later, in April 2018, the UK Serious Fraud Office (SFO) announced ‘a significant upgrade to its document analysis capabilities where AI is made available to all of its casework’.⁹

With governments and regulators embracing AI and machine learning in their respective processes, it is no surprise that they will expect corporates, legal counsel and forensic accountants to deploy AI and machine learning where it is suitable to do so in investigations and compliance programmes. Such proactive reporting is also considered by regulators in the determination of a penalty and negotiation of a settlement agreement (eg, deferred prosecution agreements (DPAs)).

6 <https://www.law.com/almlID/4f9981cf160ba0480300001f/?slreturn=20190618190713>.

7 <https://www.justice.gov/opa/press-release/file/1097546/download>.

8 <https://www.lawgazette.co.uk/practice/high-court-backs-predictive-coding-in-first-contested-case/5055377.article>.

9 <https://www.sfo.gov.uk/2018/04/10/ai-powered-robo-lawyer-helps-step-up-the-sfos-fight-against-economic-crime/>.

Treading carefully

Certain precautions should be taken when implementing AI for investigations. First and foremost, be prepared to provide the enforcement agencies and regulators with details, including:

- why it was deemed appropriate to utilise AI as part of the investigation approach;
- the type of AI (technology) deployed;
- the data sources that were incorporated and examined;
- evidence of the robustness and thoroughness of the process; and
- evidence of oversight and quality control processes.

Most enforcement agencies and regulators encourage corporates and their legal counsel to have open dialogue to allow them to understand the investigation approach and AI technology deployed. The onus is on corporates and their legal counsel to ensure that the method is sufficiently robust and defensible in a legal proceeding, and to ensure that it is duly explained to the enforcement agencies and regulators. Failure to do so may lead to the results of the investigation being discredited or deemed not admissible for legal proceedings.

Corporates and their legal counsel should also be wary of the fact that regulators often have access to multiple sources of information and data during the course of an investigation. It should be assumed that regulators will use such information and data to cross-check and validate the quality of the AI output and methodology deployed.

Benefits of AI in investigations and compliance programmes

There are many benefits in deploying AI in investigations and compliance programmes. Advocacy by the legal courts and willingness by both corporates and practising professionals to adopt AI in investigations suggest that the benefits are appreciated and welcomed, which is likely to propel further advancement of this type of technology in the near future. Benefits include the following.

Making use of large volumes and different types of data

AI provides a solution to cope with explosion of data through effective sorting of both structured and unstructured data sources (eg, text, emails, audio files, videos, etc).

Where systems operate in silo, AI also enables information and data sets to speak to one another, which in an investigation can be a Herculean task. AI allows the application of learnings from the review of unstructured data to the analysis of structured data, the normalisation of data and the identification of patterns and anomalies – all of which ease the work of an investigator.

Increased accuracy

AI has the ability to predict behaviour based on pattern recognition. Back propagation and self-learning algorithms mean that the process is repeatedly being fine-tuned until it reaches a point where the output is the most relevant, and noise and false positives are significantly reduced.

Increased efficiency

Methods such as robotic process automation (RPA) and optical character recognition (OCR) reduce the amount of manual work to a bare minimum, thereby reducing potential human errors and also reducing processing time as it is not dependent on human resource. TAR, on the other hand, hones in on the most relevant documents in a short space of time and focuses the investigator's review on the key documents only, thereby eliminating a significant number of the false positives.

Reduction in cost

Once the AI process is designed and tested, the cost and manpower required to operate the process during an investigation is significantly reduced. Human intervention is therefore concentrated squarely on assessing the appropriateness of the output.

Removal of sensitive information

Data privacy laws and regulations are on the rise globally and they are a minefield to navigate. Investigations need to comply with laws and regulations relating to data handling. Algorithms can be designed to whittle out information or data that may potentially be personal data or national or state-sensitive information, such that no human reviewers ever see such information.

Consistent and defensible

A tried and tested AI process can be deployed across various investigations and compliance programme reviews, with only key case-specific parameters requiring modification. The process eliminates human assessment, reducing the margin for inconsistencies (eg, where members of a team of reviewers do not tag documents reviewed in the same way) and human error. As mentioned earlier, the process is traceable and consistent to an extent that human effort alone could not produce.

Challenges

AI and machine learning are not foolproof and the deployment of such technology on investigations is not without its challenges.

Readiness

As with other aspects of technology advancement, the perennial question of 'are we ready?' arises. Those who do not fully understand the process may find it daunting and therefore shy away from deploying AI in investigations and compliance programmes.

Time-consuming

Deployment of AI enables an increase in overall efficiency. However, it is important that the design of the AI process is done appropriately and the design is fine-tuned to churn out accurate results.

Respecting data privacy

Technical data experts and experts in data privacy need to collaborate right from the get-go to ensure that laws and regulations are not breached in the deployment of AI in investigations.

Knowing the limits of technology

The facts behind each investigation are unique and each situation is dynamic, which means that there are multiple moving parameters to consider and integrate to develop a comprehensive AI approach.

To develop a useful and reliable system that is able to cope with dynamic and complex investigations, large volumes of good quality data are required to be able to train AI to incorporate those learnings back into the algorithm. For highly complex investigations one might also need to design many rules and exceptions for the system, which may become too large, complicated and unwieldy for the system to process.

Last but not least, AI has not (yet) surpassed human intuition and therefore requires experienced investigators to assess and ensure that the appropriate data is collected and the right questions are answered.

Conclusion

AI and machine learning are very much here to stay – while technology creates the issue of voluminous data, it also provides the solution. As we have seen with the passage of time and with our increased reliance on technology, AI will become a necessity rather than a luxury, and the volume of corporate data will amplify the need for more efficient corporate investigative tools.

To maximise the benefits of AI in investigations, investigators and compliance professionals will need to be flexible in adapting their approach to cope with the sheer volume of data, while striving to be as efficient as possible. Furthermore, with the increase in cross-border multi-jurisdictional investigations, relevant data privacy laws will have to be taken into consideration during the design stage of the AI process prior to deployment on the investigation. AI also sees the need for closer collaboration between data experts, lawyers, forensic accountants, investigators and compliance professionals to ensure proper and successful integration of AI into investigations and compliance programmes.

From a purely economic angle, it is inconceivable at this stage to revert to the expensive analogue days of linear search review to tackle the mountain of data we have today. AI is unlikely to completely replace human evaluation and critical thinking, but machine learning should sit alongside and enhance the human decision-making process.



Weng Yee Ng
Forensic Risk Alliance

Weng Yee Ng is a director at Forensic Risk Alliance (FRA). She holds more than 16 years of experience in external and internal audit and forensic accounting. Her expertise includes compliance reviews, internal investigations, litigation support (both civil and criminal), risk assessments, evaluation of compliance programmes Foreign Corrupt Practices Act monitorships for both the Department of Justice and the Securities Exchange Commission, disgorgement and penalty calculations, procurement fraud matters and third-party due diligence.

Weng Yee is currently working on a risk assessment and evaluation of compliance program for an aviation company. She has recently completed compliance monitorships for a medical devices company and for a financial transaction systems manufacturer, both with global presence, a proactive anti-bribery and corruption review for an international bank and several internal investigations into whistleblower alerts for a CAC 40 automotive original equipment manufacturer.

Having spent over six years working in-country in Malaysia, Weng Yee possesses a first-hand understanding of the business nuances and financial and reporting practices encountered in Malaysia and in other Southeast Asia countries. She is multilingual in English, Malay, Cantonese and Mandarin, and is familiar with Bahasa Indonesia and Spanish.

Weng Yee is recognised in *Who's Who Legal: Investigations Forensic Accountants, Consulting Experts* and *Global Elite*.



James Norden
Forensic Risk Alliance

James is a manager in FRA's forensic accounting team in London, with more than seven years of experience in external audit and forensic accounting. He joined FRA in 2016, after four years at BDO LLP in their financial services external audit practice. He is an ACA chartered accountant (ICAEW).

At FRA, James has chiefly worked on a large-scale internal investigation for an aviation company, a corporate compliance monitorship of an international bank for the US Department of Justice, as well as a proactive anti-bribery and corruption review for another international bank. In each case, he reviewed business activities and transactions on a global scale, with touchpoints in APAC, the US and the Middle East. James has also worked on investigations and compliance reviews of two separate multinational companies in the medical devices sector, including in-country reviews and interviews in India and Eastern Europe.

At BDO, James focused on the financial services sector, including audits of asset managers, banks, and a FTSE 250 listed private equity house. On secondment to BDO USA, he led venture capital fund audits in the San Francisco Bay Area.

James graduated with an honours degree in history and German from Durham University, England, including a year abroad at the University of Cologne, Germany. He is fluent in German.



Forensic Risk Alliance (FRA) is a global market leader working with clients to identify, analyse, and mitigate the risks associated with international regulatory compliance obligations, litigation, internal and external multi-jurisdictional investigations. Unlike traditional accounting firms, we operate purely in the forensic space and generally have no conflicts. Our highly skilled and sophisticated team comprises forensic accountants, former investment bankers, financial and data analysts, legal and litigation support professionals, database architects, electronic discovery and collection experts, software engineers, and certified computer examiners. This includes individuals who have worked for the UK Serious Fraud Office, US Securities and Exchanges Commission, and US Federal Bureau of Investigation.

As internationally recognised specialists in multi-jurisdictional investigations, we bring a high level of confidence to clients by providing clear, robust and candid advice that is trusted by clients, regulators, courts and enforcement agencies.

We have extensive cross-sector and cross-border experience and scalability anywhere in the world. Our globally integrated teams have worked in more than 75 countries – both developed economies and emerging markets.

We offer extensive data privacy and protection and jurisdiction-specific experience (eg, blocking statutes, banking and state secrecy laws, commercial secrecy, global privacy legislation and security risks, state sponsored and other hacking, leaks, data loss and excessive data retention).

Complex data analytics, information technology and data management are at the core of our foundation. Our data analytics team seamlessly integrates with our forensic accounting, digital forensics and eDiscovery teams to offer creative analytical and visualisation solutions tailored to client needs.

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

Weng Yee Ng
wng@forensicrisk.com

James Norden
jnorden@forensicrisk.com

www.forensicrisk.com

The *Asia-Pacific Investigations Review 2020* contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.