Global Investigations Review

The Guide to International Enforcement of the Securities Laws

Editors
John D Buretta, David M Stuart and Lindsay J Timlin

The Guide to International Enforcement of the Securities Laws

Editors

John D Buretta

David M Stuart

Lindsay J Timlin

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2021
For further information please contact insight@globalrestructuringreview.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at November 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-597-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

BLAKE, CASSELS & GRAYDON LLP

BOUGARTCHEV MOYNE ASSOCIÉS AARPI

CORRS CHAMBERS WESTGARTH

CRAVATH, SWAINE & MOORE LLP

DLA PIPER

FORENSIC RISK ALLIANCE

GLEISS LUTZ

HERBERT SMITH FREEHILLS NEW YORK LLP

KIRKLAND & ELLIS LLP

KOBRE & KIM

LENZ & STAEHELIN

MARVAL O'FARRELL MAIRAL

MILLER & CHEVALIER CHARTERED

S&R ASSOCIATES

SLAUGHTER AND MAY

WHITE & CASE LLP

WIELEWICKI, MAIA & TROVO ADVOGADOS

Publisher's Note

Global Investigations Review is delighted to publish *The Guide to International Enforcement of the Securities Laws*. For those who don't yet know, Global Investigations Review is the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell them all they need to know about everything that matters.

GIR is famous for its daily news, but we also create more in-depth content. It includes a technical library, a volume of which you're now reading; full reporting of the liveliest conference series in the white-collar world, GIR Live (our motto: 'less talk, more conversation'); and unique data sets and related workflow tools to make daily life easier. And much else besides.

Being at the heart of the corporate investigations world, we often become aware of gaps in the literature before others – topics that are crying out for in-depth but practical treatment. Recently, the enforcement of securities laws emerged as one such fertile area.

Capital these days knows no borders, but securities-law enforcement regimes very much do. In that juxtaposition lie all sorts of questions. The book you are holding aims to provide some of the answers. It is a practical, know-how text for investigations whose consequences may ring in securities law. Part I addresses overarching themes and Part II tackles specifics.

If you find it helpful, you may also enjoy some of the other titles in our series. *The Practitioner's Guide to Global Investigations* is the best known. It walks the reader through what to do, and consider, at every stage in the life cycle of a corporate investigation, from discovery of a possible problem to its resolution. Its success has spawned a series of companion volumes that address monitorships, sanctions, cyber-related investigations and, now, securities laws. Please visit the Insight section at www.globalinvestigationsreview.com to view the full technical library. GIR subscribers receive a copy of all our guides, gratis, as part of their subscription. Non-subscribers can read the e-version at www.globalinvestigationsreview.com.

I would like to thank the editors of *The Guide to International Enforcement of the Securities Laws* for helping us to shape the idea. It's always a privilege to work with Cravath, Swaine & Moore. I'd also like to thank our authors and my colleagues for the elan with which they've brought the vision to life.

We hope you find it an enjoyable and useful book. If you have comments or suggestions please write to us at insight@globalinvestigationsreview.com. We are always keen to hear how we could make the guides series better.

David Samuels
Publisher, GIR
November 2021

Contents

Part II: Expert International Perspectives

Part I

Overview of International Enforcement of the Securities Laws

6

Forensic Procedures in Securities Investigations

Frances McLeod, Jerry Hansen, Neil Keenan and Alejandro Gomez-Igbo[1]

Common types of securities-related investigations and related forensic procedures

Each investigation is unique in many respects owing to the nature of the alleged wrongdoing, the jurisdiction involved and the company's industry; however, there remains a basic framework applicable to most investigations, including some common processes and procedures. Most forensic investigations have the following key elements:

- a triggering event;
- a preliminary analysis;
- planning and coordination;
- discovery of data and other evidence;
- interviews;
- compilation and analysis of facts;
- conclusion of findings; and
- reporting of findings, recommendations and remediation.

Most of these elements will be repeated during an investigation as allegations are clarified and additional information is assessed resulting in additional planning, discovery, interviews and analysis being performed.

An essential element of an investigation is the preservation, collection, processing and review of evidence, the vast majority of which is in electronic form. In this chapter, we discuss some common features and key considerations when undertaking this aspect of an investigation, and the challenges that can arise from relatively recently enacted privacy laws, blocking statutes and state secret acts. Another essential element is interviews conducted throughout

1 Frances McLeod is the founding partner, Jerry Hansen and Neil Keenan are partners and Alejandro Gomez-Igbo is a director at Forensic Risk Alliance.

an investigation. Not only do they act as a means of gathering valuable information but they also provide investigators with important 'mental impressions' of what was said or inferred by the interviewee, what was not said and the overall demeanour (e.g., body language) of the interviewee. A well-constructed interview requires both skill and experience and it is important to develop an interview strategy that considers the sequencing of individuals to be interviewed, the timing of interviews and clear objectives for each individual interview.

Successful interviews focus on the knowledge and facts that the interviewee would, or should, be in possession of. For example, C-suite executives may have a strong understanding of the business objectives, trends, customers, operations and overall financial performance and targets, but will not likely have detailed knowledge of individual transactions, contracts, agreements or relationships. Such knowledge will most likely reside with key accounting personnel, sales and account managers, local procurement personnel and warehouse personnel. To form a more comprehensive picture of what occurred, it is essential to complete the puzzle by combining the pieces provided by various levels within the organisation. It is common practice – and advocated by many global enforcement agencies – to commence interviews from the ground up, gathering information from those most knowledgeable of individual transactions, vendors, customers or relationships, that can then be used to inform and prepare for interviews of more senior personnel.

Beyond the investigation, other considerations must be addressed to fully resolve a matter, including the remediation of compliance and internal control gaps, weaknesses and failures and, where applicable, the resolution of investigations by government prosecutors and regulators. Resolving investigations by prosecutors is complex as they involve many potential elements, including: interpretation of the underlying facts; violations of securities laws that have or may have occurred; the level of fines, penalties and disgorgement of ill-gotten gains; and the potential appointment of a compliance monitor.

In this chapter we consider some of common securities-related investigations and techniques that can be deployed, including data collection and processing considerations. We also discuss best practices when presenting to enforcement agencies and regulators.

Accounting-related fraud

While perhaps not as prevalent as in the early part of this century, accounting fraud remains a focus of global enforcement agencies. When accounting fraud occurs, it can have a significant impact on shareholders, company customers and vendors, and overall market confidence. Large-scale accounting cases remain, with notable recent examples involving NMC Health plc, Finablr plc and Wirecard AG.

Motives for committing financial-related fraud can be widespread, ranging from increasing the value of company shares and stock options, to the need to meet analyst expectations, or to obtain necessary increases in funding through equity or debt providers. However, corporations do not commit fraud – fraud schemes are perpetrated by individuals within the company, frequently with the assistance of outside third parties. It is important when investigating such misconduct to identify the personal motivations of individual employees, such as: promotion and advancement; bonus and increased compensation; stock options and stock incentive plans; and personal egos and standing in the community.

The most common accounting-related fraud schemes involve intentional acts resulting in:

- overstatement of revenue and assets;

- understatement of expenses and liabilities;
- inaccurate application of accounting estimates;
- misapplication of generally accepted accounting principles; or
- false statements or omission of information material to the users of financial statements.

Several of these schemes can arise from manipulating the timing of when transactions are recorded or when certain key events transpired. They very often start off small, with the fraud occurring to rectify a short-term deficit in a company's earnings. Accelerating revenues or deferring expenses in the current quarter can enable the company to meet or exceed analyst expectations, with the thought being that the business is expected to pick up in the subsequent quarter so the entries can be reversed and nobody will be harmed. When the uptick in business fails to materialise, however, the fraud often needs to continue to hide the activity. Over time it can grow significantly, becoming increasingly complex and resulting in a greater chance of it being discovered.

Techniques for investigating revenue schemes

A revenue scheme involving the posting of fictitious sales is relatively straightforward to orchestrate but can initially be challenging to detect. By nature, such sales are not real and fraudsters must deploy means to conceal the fact that no cash will ultimately be received. This is where investigators can uncover such schemes. A detailed analysis of accounting records and data in the following areas can reveal trends that highlight potential fictitious sales:

- cash receipts: a review of cash receipt activity can identify if cash is being misallocated to other customer accounts, or other invoices within the same customer receivables balance, thereby falsely recording the settlement of the fake invoices (a scheme known as lapping);
- write-offs: large write-offs of customer account balances that are unsupported by legitimate cash collection efforts can be an indicator of inappropriate activity; and
- unusual accounting entries: entries that transfer a receivable balance to another asset category where there is no expectation of being collected (e.g., prepayments, inventory), or to offset a liability, can indicate possible management of earnings.

Cut-off schemes are well known to enforcement agencies and most often involve a company recognising revenue on genuine sale transactions, but prior to such revenues being 'earned' in accordance with the relevant accounting guidance. Cut-off scheme fraud is often perpetrated by:

- entering into 'side agreements', written or oral, with customers whereby the company agrees not to enforce contractual arrangements until certain later dates (or provides a right to return unsold products);
- shipping products to customers before the order request date;
- shipping products to intermediate holding locations rather than the customer; or
- amending shipment terms so the customer takes ownership of the goods at shipment versus delivery.

Documents may be manipulated, amended, backdated or otherwise altered to document the transaction under terms inconsistent with the actual agreement with the customer. Investigative techniques will frequently involve:

- data analysis on sale trends, including timing of large-sale transactions at the end of the quarter and evidence of financial records being left 'open' to record sales after the actual quarter close;
- reconciliation of the timing of transactions in the accounting system (structured data) to what was actually occurring at the transaction date, often obtained through interviews combined with a review of emails, customer correspondence or other forms of unstructured data;
- review of changes in credit terms on customer accounts, including for specific invoices; or
- analysis of subsequent returns of products, issuance of credit notes to customers that can be offset against future purchases, or write-offs of receivable balances of quarter end sales (or all of these).

The investigative techniques previously discussed can also assist in discovering other revenue fraud often perpetrated with the assistance of a third party. One example is 'channel stuffing' whereby a company oversells goods to its agents and distributors with the understanding that goods can be returned or payment terms will be extended until goods are ultimately sold. Another example is 'round-tripping', where two parties agree to procure each other's goods under a reciprocal agreement. Round-trip transactions can often be identified through the analysis of sale and procurement transaction documents for identical or similar amounts, executed at the same time, especially those with cash not being exchanged between the two parties, resulting in the receivable and payable balances being offset.

Techniques for investigating earnings management

With public companies commonly announcing earnings per share targets, coupled with analysts' expectations, there is pressure on public companies to meet or exceed such expectations to maintain the stock price, meet bonus targets and other incentives that can yield significant benefits (or avoid significant negative impacts) to company officers. Given the potential benefits, it is not surprising that managing earnings through fraudulent means has been a part of numerous enforcement actions.

While there are many ways that companies can manage earnings, a common method is the intentional misapplication (i.e., manipulation) of accounting estimates. Accounting estimates are an appropriate and necessary part of preparing financial statements and include, for example, allowances for doubtful debts, inventory reserves, impairment of long-lived assets, sales returns and warranties, and contingent liabilities, to name a few.

Financial fraud involving the manipulation of accounting estimates is investigated through the following techniques:

- assess, over time, the consistency of the methodology applied by management to determine accounting estimates, including the basis of the calculation, the source of the data used and whether any current developments render historical practices insufficient or invalid;
- determine whether factors that could impact the estimate are intentionally omitted (e.g., if, as part of a new sales campaign, increased warranty periods are offered but these increased periods are not factored into the estimate calculation);

- consider the integrity of data used to form estimates to confirm that it has not been doctored or amended (e.g., amended historical warranty or right of return data to 'justify' a lower warranty provision);
- through a review of emails, interviews and general business trends assess whether assumptions used do not accurately reflect management's true knowledge and belief at the time the estimates are made; and
- assess and recompute estimates to ensure that the mathematical model calculations are accurate and factor in all required inputs and assumptions, and that such inputs and assumptions are accurate.

Techniques for investigating disclosure frauds

Public companies are required under securities laws to provide investors with copious amounts of information from financial statements and associated footnotes, management discussion and analysis that covers business operations, press releases, and earnings announcements and calls. Disclosure fraud can arise from making knowingly false or misleading statements or intentionally omitting materially relevant information. Disclosures by companies are heavily scrutinised and hindsight is often applied to question historical statements, leading to investigations and possible enforcement actions. Investigating disclosure fraud cases primarily involves the assessment of what management knew, or ought to have known, at the time the disclosure was made and whether this was consistent with the public statements released. This, therefore, requires the investigator to:

- understand the disclosures made, the data and assumptions underlying the disclosures in question, and the individuals who assisted in assessing, drafting and approving the disclosures;
- assess the integrity and accuracy of the data and assumptions used by management, often accomplished through data analytics, recalculations and validity of source information; and
- compare and contrast the underlying assumptions with what individuals knew or thought at the time assumptions were created, typically obtained through a review of general business or industry trends, email correspondence and interviews.

Corruption

During the past two decades, enforcement agencies have prosecuted numerous companies that engaged in corruption and the subsequent penalties, fines and disgorgement of ill-gotten gains have been substantial. Corruption investigations are typically multifaceted and can take considerable time and effort to complete. The complexity arises from both the nature of corrupt payments and the frequency with which they are made, and the fact that many corruption cases are international, often in several different jurisdictions, meaning access to data and individuals requires careful consideration to avoid tripping over data privacy and other related regulations specific to the countries involved.

Corruption, as defined in various international laws, can take many forms, some of which are easier to investigate than others. For example, allegations related to lavish entertainment and gifts, donations to charities and hiring of relatives of government officials are more straightforward. Such transactions can typically be quantified and traced within accounting and corporate records. Assessing the business purpose, the ultimate recipient and the 'benefit'

obtained by the corporation, however, can be more complex. Corruption schemes involving kickbacks to secure contracts can increase the level of complexity as they commonly involve the use of third parties (e.g., agents) and are recorded as apparently genuine transactions within the company's books and records. Investigation techniques seek to gather circumstantial evidence that suggests that payments may not be for the stated purpose and ring-fence the issue through document review and interviews, thereby 'boxing in' those involved in the scheme. While each investigation differs, some common techniques include the following:

- data analytics and research on third-party suppliers, including the amount and frequency of payments, the timing of payments relative to key project milestones, one-time vendor payments, and spending on higher-risk service providers versus those delivering physical goods;
- evaluating the company's compliance with its own internal policies and procedures, including procurement controls around sourcing and vendor identification, the number of bids and tenders, the vendor evaluation and selection processes, vendor due diligence procedures, contracting (including payment terms), and purchase order and invoice processing;
- background research into higher-risk vendors, including ownership and management, relevant skills and resources, a track record of similar project delivery, and reputation and past allegations of misconduct;
- for higher-risk vendors, assessing the reasonableness of their role on the project, the suitability to perform the requested services, the reasonableness of the fees charged, the transparency of the work performed and the deliverable provided (this can be performed through a review of invoices and supporting documents, correspondence with the vendor, review of deliverables and interviews of company employees involved in the management and delivery of the project);
- reviewing commissions and bonuses paid to third parties and company employees to assess those who may have personally benefited from the contract award; and
- reviewing emails using tailored search terms and the chronology of the project (e.g., request for information, request for proposal, bid submission, commencement date, significant change order submissions and acceptance, and milestone payments).

Money laundering

Money laundering involves the transfer of funds that are the proceeds of illegal acts, the transfer of unreported funds (above specified monetary limits) or the transfer of funds not in compliance with the relevant country's banking laws. Although money laundering is a diverse and often complex process, it generally involves three stages: placement, layering and integration. Those investigating allegations of money laundering benefit from the fact that money laundering transactions have a digital footprint with virtual and physical connections. Analysing data and making connections between different bank accounts and individuals or corporations is the cornerstone of such investigations. Investigative techniques include:

- extraction and analysis of customer, transaction and monitoring alert data;
- in-depth public record research of high-risk customers and persons of interest to identify personally identifiable information that can be used to link individuals, accounts and corporations – such attributes will include the person's or corporation's name, age,

address, email address, employer, corporate ownership, family members and any accounts with the institution;

- use of data analysis techniques to detect the initial placement of funds – these techniques seek to identify deposits that are:
  - large cash sums with little known about the origin of the cash;
  - small-value amounts with high frequency; or
  - inconsistent with the business that is alleged to have generated such funds;
- identification of layering patterns through 'flipping transactions' or round-trip transactions between entities that appear to lack a legitimate business purpose – appropriate analyses would identify large, frequent transactions between the same accounts (or a number of common accounts) for similar amounts on and around the same dates;
- investigation of extraction patterns through a review of accounts that appear to control the transaction flows inside a complex interconnected transaction network; and
- a focus on internal controls implemented at the institution, including customer onboarding, background checks, know your customer processes, red flag testing procedures and suspicious activity reporting.

Data governance considerations in forensic procedures

Data scope

Identifying the data scope is often one of the first steps of investigations and involves determining the location and format of the various types of electronically stored data. At this stage, it is advisable to review allegations, agree upon the period of review, understand the jurisdictions involved and, most importantly, determine the relevant custodians.

Once the scope and jurisdictions of data to be reviewed have been decided upon, the second step is to perform data collection. At this stage, many teams can be involved in discussions with company management and IT personnel at different levels and business locations to get a better idea of the type of data, and where and how it is stored, and understand any possible issues prior to collection. There can be varying methods for capturing different information, depending on the type of data, and the owner of the data or device, including mobile phones and tablets owned by employees. The main goals are to avoid a re-collection (due to any gaps in the data set) and to find a good balance between the amount of data captured and the time and cost spent on collection.

Structured and unstructured data review

Once collection and processing of data is complete, it can be prepared for review, but consideration is required with regard to whether the data is structured or unstructured. Unstructured data is data that is not organised in any predefined manner and, as such, can be harder to review and analyse. Examples of unstructured data are chats, audio, text messages, video and social media logs. Structured data is made up of defined data types that are organised in tabular formats (rows and columns), and is highly organised and formatted, making it more easily searchable. Examples include ERP accounting data, transaction records and Excel files. Semi-structured data has a hybrid of both structured and unstructured elements; email data falls under this category. While the actual content of the email is unstructured, it does contain structured data such as the names and email addresses of the sender and the recipient,

and the date the email was sent. Reviews should use analytics to identify potentially relevant (or eliminate irrelevant) documents to inform the investigation team.

It is important to identify the available structured and unstructured data that might be useful to the investigation and assess how best to combine, process and search such information. Organisations must understand the nuances between both types of data to best assess how these data sets are governed, preserved and extracted for investigative purposes.

Data hosting considerations

Data hosting solutions can vary depending on data volume and type, and require a concrete understanding of the data to be collected. The data management team will need to assess the technology and data search strategies required. Not all data collected will be reviewed; therefore, processing and hosting only the relevant data presents a more cost-effective solution.

It is important to consider the jurisdictional restrictions regarding data and whether the collected data is allowed to leave the premises of the site where it was collected. For instance, as soon as the data leaves the office building without permission from the custodian of the data, it could be subject to security and privacy breaches. The isolation of some data from other data is called air locking, which isolates data in a 'quarantine' state called the air gap. The air gap allows data to be analysed outside a larger network, adding increased safety against cyberattacks and other malware infecting the main network.

Such challenges are often best handled by mobile solutions, since data remains on the premises and typically requires the review to be completed by professionals with a national security clearance depending on the sensitivity of the information. Due diligence in this regard is necessary to allow the investigative process to remain compliant. If data cannot be moved outside the firm's premises or the host country, a mobile review solution can be implemented for the investigation. Mobile review solutions provide 'air-gapped', end-to-end processing, review and document production platforms and can be used to avoid cross-border issues and data security breaches.

Cloud-based solutions for data hosting are becoming increasingly widespread, propagated further by the rise of remote work as a result of the covid-19 pandemic. If such a solution could be used it would allow investigation teams to consider a range of cloud-based storage options and find the one that would best satisfy the needs of the investigation. Cloud-based solutions allow for large volumes of data to be stored, which can be accessed from different devices.

Complex data issues and solutions

New messaging tools

The use of handheld technology is prevalent globally, both in personal and in professional settings. Not only has the use of personal communication tools emerged as a catalyst for dialogue and collaboration, but the abundance and diversity among various providers have contributed to their widespread use. Providers such as WhatsApp, Facebook Messenger, Microsoft Teams, Slack, Zoom and other social media applications have all emerged as valuable tools throughout the twenty-first century, and have become ever-more reliable during the covid-19 pandemic. While it is fairly simple to track basic statistics on applications such as user counts, engagement and geolocation, it is significantly more difficult to analyse

individualised content. In this expanding environment for data forensic teams and investigators, novel legal challenges arise related to how to capture and preserve such data.

Significant challenges stem from both the diversity of communication platforms and the sheer volume of data they produce. Because each provider tends to be different, separate approaches must be taken with each. Some may be easier to analyse than others, such as Zoom and Slack, which are easily collected as a result of all data residing in the cloud. This data can be extracted (provided the organisation has the correct licensing) and reviewed, provided the processing software was properly deployed. The review of such data, however, can be more difficult in practice, as emerging communications providers format their data differently, which in turn may require processing software to be edited to incorporate different providers' unique data. This can lead to additional compliance risks, as it is generally uncommon to have copies of conversations downloaded onto a company server, thus systems such as WhatsApp and Telegraph would require direct access to an employee's device.

Potential solutions

Modern issues require innovative solutions. One of the potential solutions for dealing with these application-related unstructured and structured data sets is the use of active learning technology and machine learning. Within electronic discovery, active learning goes by a few names, but one of the most common on the review end is technology assisted review (TAR). An increased reliance on machine learning can allow for quicker and more decisive review metrics, by speeding up the review process, as well as yielding more relevant results. Although still in its infancy, TAR solutions are beginning to gather steam in the industry.

While new techniques and solutions are valuable, it is vital that any tools employed in an investigation are compliant with relevant laws and regulations. By discussing the approach with the relevant regulatory or enforcement agency, it is possible to minimise the risk of having to re-collect or re-process data. It is important to understand the data-related issues, including data privacy (discussed further in the next section), that will aid the investigation team in creating a customised approach using the best solutions.

Legal roadblocks to performing certain procedures

Emerging data privacy concerns

It is crucial for the investigation team to consider the relevant national and international data-related legal provisions when conducting an investigation. The required data is not always located in one jurisdiction; therefore, before a data transfer is performed, necessary due diligence needs to take place with respect to the relevant data privacy laws. In addition, all investigations require careful handling of personal data, including any personal identifiable information, which may require redactions. Further complicating the matter, multi-jurisdictional investigations may require more advanced security procedures to comply with blocking statutes and country-specific data privacy and security laws. Compliance with these laws will be necessary at all stages of the process, including data collection, migration, security and privacy. Failure to comply can lead to significant penalties and fines for the violator.

General Data Protection Regulation and other privacy laws

In the European Union (EU), the handling of data needs to be performed in accordance with the General Data Protection Regulation (GDPR). The GDPR, which took effect in 2018, is the main regulation for organisations in the EU, and is intended to protect the personal data of persons based in the EU. The GDPR and other data privacy regulations present additional challenges with regards to the transfer of data. Since the implementation of the GDPR, European regulators are increasing GDPR enforcement, including against companies outside the EU.

Organisations must understand that any investigation involving EU-based data carries particular challenges that should be carefully addressed. Not only is there potential for enforcement under the GDPR but data required for an investigation may be subject to unique country-specific privacy laws. To comply with data privacy (or security) protocols, clients may request that data remain on-site, which could create additional challenges for data collection and processing. Complying with the GDPR and other data privacy laws, such as the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), makes it possible to ensure that the highest level of adherence to data privacy is maintained throughout the data collection and analysis process.

State secret concerns

Several governments have passed legislation that prohibits information considered sovereign state secrets from being exported outside country boundaries. Companies must comply with such laws. In the investigation context, this requires a proactive review of relevant documents for state secret information and the exclusion of those documents so they are not exported overseas. State secret reviews require knowledge of the organisation's security policy as well as local jurisdictional provisions. For instance, certain data could be considered 'government sensitive'. In the United Kingdom, this is outlined in the government's 'Official-Sensitive' guidance on handling sensitive information in IT. It can be the case that a data transfer is not possible from a given jurisdiction if it happens to contain state secret information. To avoid any potential penalties, the data will have to remain within the jurisdiction for review. A prominent example is China's state secret laws, which present compliance challenges due to the 'ambiguity of China's law, and the inconsistent way it is enforced'.[2] Comprehensive procedures and processes must therefore be developed for collecting, processing and reviewing relevant data sources to ensure that there is no export of sensitive electronic data, as outlined in China's revised Law on Guarding State Secrets.

Blocking and localisation statutes

For investigations potentially involving the transfer of data across national borders, the team must be aware of key European legislation, known as blocking or localisation statutes, that may restrict the transfer of data. Such statutes are intended to protect the commercial interests of the country, including perceived extraterritorial interference by other countries, such

2 Megan Zwiebel, 'Six Things About State Secrets to Consider When Engaging in Internal Investigations in China (Part Two of Two)', Anti-Corruption Report. https://www.anti-corruption.com/2568711/six-things-about-state-secrets-to-consider-when-engaging-in-internal-investigations-in-china-part-two-of-two.thtml.

as US antitrust and trade sanctions enforcement. These statutes can have implications for internal and external investigations. For example, it is not unusual for an organisation to be caught in a catch-22 situation in which it is compelled by a US court order or a regulator's subpoena to disclose information that is on servers in the EU, but is prevented from transferring the information by a governing blocking statute. This is but one example of situations that may arise related to blocking statutes, highlighting the fact that investigations should be aware of such regulations and the related issues they may present.

Presenting results of forensic procedures to regulators

For many securities-related investigations, the presentation of the results of the investigation will be required. When informing regulators of an investigation, including its scope, findings and conclusions, questions from regulators often include the following:

- Did the company commit to learn the truth, fully and expeditiously?
- Did the company perform a thorough review of the nature, extent, origins and consequences of the conduct and related behaviour?
- Did management, the board or committees consisting solely of outside directors oversee the review?
- Was the investigation performed by external counsel and advisers that demonstrated appropriate objectivity?
- Did the company promptly make available the results of its investigation and provide sufficient documentation regarding its response to the situation?
- Did the company identify possible misconduct supported by evidence with sufficient precision to facilitate prompt enforcement actions against those who violated the law?

The timing of disclosures to enforcement agencies is complex and requires a balance between early disclosure while ensuring that adequate information has been determined to make disclosures meaningful and informative. Early discussions will focus primarily on:

- the nature of the alleged misconduct;
- the origin of the allegations;
- the structure of the investigation team;
- the scope of the investigative work, including the retention, collection, processing and review of electronic and hard-copy documentation; and
- the timing of future investigative work.

In addition, an increasingly important element of such discussions is the handling of potential electronic evidence.

Electronic records

As discussed frequently in this chapter, investigations rely heavily on the review of electronic records. With global privacy laws and regulations, blocking statutes, state secret laws and, based on the industry, contractual and product confidentiality, data processing and review is increasingly complex. Providing a thorough background on how the investigation has or is capturing and processing data, including any restricted data sets, is essential to increase an enforcement agency's confidence that appropriate steps have been taken.

How the investigation team reviewed large data sets is also important to the regulators who may wish to 'audit' how the review was conducted. Where restricted data sets are subject to various levels of culling prior to being reviewed by the primary investigation team, regulators will want to understand how the review was filtered, and what checks were performed to validate that all information relevant to the investigation was made available for review. Further, when artificial technology or TAR tools and techniques are used to streamline the review of large data sets, investigators should provide detailed explanations of how such techniques were applied and what testing was done to validate the effectiveness, and be prepared for enforcement agencies to challenge and audit such processes.

Presentation of findings and observations

When presenting the findings of an investigation to an enforcement agency, an essential element is the accurate and complete presentation of the facts and evidence as discovered. Regulators, however, do often allow counsel to provide an alternative but objective interpretation of the facts. This can involve completing different forms of, for example, creative analysis and insights to fill in gaps in the information, or providing potential motives for individuals involved in the alleged misconduct. The most appropriate means of communicating with enforcement agencies will vary based on the underlying misconduct and the complexity of the issue; however, common techniques to present findings include the following.

- A PowerPoint presentation is prepared that provides a high-level summary of the scope of the investigation, the key findings and the primary sources of evidence that support such observations. The PowerPoint will be supplemented with oral presentations and the most relevant or 'hot' documents that support the investigators findings (e.g., emails, text communications, contracts, invoices and other accounting records).
- When presenting accounting-related data, data visualisation tools are used to simplify the presentation of large data sets.
- Presentations include the lead counsel conducting the investigation, supported by forensic accounting and data specialists. Consideration should also be given to company representatives to permit the enforcement agency to hear directly from the corporation.

Investigation teams should be prepared to answer questions and resist the temptation to defer or 'get back to' regulators later. Pre-empting potential questions and having appropriate and accurate responses ready will provide greater comfort to enforcement agencies that the investigation team has a robust understanding of the events and circumstances under investigation and are engaging in a cooperative and open discussion.

Finally, corporations should proactively describe the remediation measures that have been taken. Regulators have publicly stated that they view favourably companies that recognise that weaknesses existed in the internal controls environment and took steps to remediate such deficiencies in a timely manner.

Appendix 1

About the Authors

Frances McLeod
Forensic Risk Alliance

Frances McLeod is a founding partner of Forensic Risk Alliance (FRA) and is head of its US offices. She is a former investment banker and has over 25 years of experience advising diverse clients on sanctions, anti-corruption, fraud, internal controls, asset tracing and money laundering issues.

Frances has been deeply involved in all of FRA's compliance monitorship work, both serving as the monitor and supporting the monitor, including US Department of Justice and Securities and Exchange Commission FCPA monitorships, a New York Department of Financial Services bank monitorship, the Ferguson City monitorship, a Public Company Accounting Oversight Board monitorship and a Department of Justice fraud-related monitorship with an environmental compliance element.

Frances has extensive experience in addressing complex international data-transfer issues whether in regulatory investigations or cross-border litigation. She led the FRA team in responding to anti-corruption investigation data requests in all jurisdictions for Alstom in the United States, the United Kingdom, Brazil, Indonesia, Poland and Sweden, among others, which included addressing French data privacy and blocking statute issues. She is leading FRA's General Data Protection Regulation compliance initiative, leveraging FRA's decades of experience in addressing data protection issues in cross-border litigation and investigation.

Jerry Hansen
Forensic Risk Alliance

Jerry Hansen is a partner based in Forensic Risk Alliance's Dallas, Texas office. He has over 25 years of experience in accounting and forensic services, including M&A disputes, audit and accounting malpractice litigation, forensic due diligence, compliance monitorships and fraud investigations.

Jerry has provided forensic, dispute and audit-related services to clients in a wide range of industries, including real estate, technology, energy, transportation, manufacturing, software, food services, publishing, automotive, healthcare, retail, staffing services, advertising, professional services and financial services. His expertise includes serving as an expert or neutral arbitrator in resolving post-closing purchase price dispute arbitrations, providing expert and consulting services in audit and accounting malpractice matters involving the application of generally accepted accounting principles and generally accepted auditing standards, conducting all manner of forensic investigations, and providing forensic due diligence services related to Foreign Corrupt Practices Act and UK Bribery Act risks. His industry experience includes software revenue recognition, mortgage banking, insurance claims and real estate.

Jerry is a certified public accountant, licensed in Texas and California. He holds a BBA in Finance from Southern Methodist University and an MS in accounting from the University of Virginia.

Neil Keenan
Forensic Risk Alliance

Neil Keenan is a partner at Forensic Risk Alliance and is based in the firm's Washington, DC office. He has considerable experience providing accounting and advisory services to clients across a variety of industries and geographies. Neil specialises in the delivery of forensic accounting services, including accounting fraud, audit and accounting malpractice litigation, anti-corruption investigations and compliance, and asset misappropriation and embezzlement. Beyond investigations, Neil brings broad experience that includes claims processing, M&A financial and compliance due diligence, corporate finance, corporate valuations, business recovery and restructurings, and external and internal audit services. Neil has a degree in chemistry from the University of Aberdeen, UK and is a member of the Institute of Chartered Accountants of Scotland.

Alejandro Gomez-Igbo
Forensic Risk Alliance

Alejandro Gomez-Igbo is a director based in FRA's London office. Alejandro's unique experience traverses both structured and unstructured data, providing a holistic strategic perspective on the collection, analysis and reporting of large quantities of multiple types of data, while leveraging the latest advanced technology offerings.

Alejandro specialises in complex data issues, primarily involving interviewing and advising clients to understand IT business processes and identifying responsive data for disclosure exercises. He has been a key player in high-profile cases and has supported and managed cases of varying sizes involving the biggest UK and US regulatory bodies.

Alejandro holds industry certifications in anti-money laundering, forensics, early-case assessment and analytics tools, and advanced visualisation software. He completed university with a BSc in business management and information systems. He is fluent in Spanish and Italian.

Forensic Risk Alliance
Audrey House
16–20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110
fmcleod@forensicrisk.com
jhansen@forensicrisk.com
nkeenan@forensicrisk.com
agomezigbo@forensicrisk.com
www.forensicrisk.com

Capital these days seems to knows no borders, but securities laws very much do. In that juxtaposition lie all sorts of challenges for those charged with investigating whether any law has been broken.

GIR's *The Guide to International Enforcement of the Securities Laws* aims to make practitioners' lives easier. Written by contributors with a wealth of experience, and edited by lawyers from Cravath, Swaine & Moore, this handy desktop reference guide seeks to address the most pressing questions in securities law enforcement.

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

an LBR business

ISBN 978-1-83862-597-9