GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

EIGHTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Luke Tolaini, Celeste Koeleveld, F Joseph Warin, Winston Y Chan

2024

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT

www.globalinvestigationsreview.com

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

ISBN 978-1-80449-273-4

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

Acknowledgements

Addleshaw Goddard LLP

Akrivis Law Group, PLLC

Anagnostopoulos

Baker McKenzie

BCL Solicitors LLP

BDO USA, PC

Bennett Jones LLP

Campos Mellos Advogados (in association with DLA Piper)

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Cravath, Swaine & Moore LLP

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Dechert LLP

Díaz Reus Abogados

DLA Piper

Eversheds Sutherland

Fornari e Associati

Fountain Court Chambers

Fox Williams LLP

Gibson, Dunn & Crutcher LLP

Goodwin

Herbert Smith Freehills LLP

Homburger

Jones Day

Kingsley Napley LLP

Kirkland & Ellis International LLP

Latham & Watkins

Law Offices of Panag and Babu

Linklaters LLP

McDermott Will & Emery UK LLP

Marval O'Farrell Mairal

Matheson

Meredith Connell

Moroğlu Arseven

Morvillo Abramowitz Grand Iason & Anello PC

Navacelle

Noerr Partnerschaftsgesellschaft mbB

Paul Hastings LLP

Rebaza, Alcázar & De Las Casas

Shearman & Sterling LLP

Skadden, Arps, Slate, Meagher & Flom (UK) LLP

Sullivan & Cromwell LLP

Travers Smith LLP

Uría Menéndez Abogados, SLP

Walden Macht & Haran LLP

Willkie Farr & Gallagher LLP

Withersworldwide

Publisher's Note

The Practitioner's Guide to Global Investigations is published by Global Investigations Review (www.globalinvestigationsreview.com) – a news and analysis service for lawyers and related professionals who specialise in cross-border white-collar crime investigations.

The Guide was suggested by the editors to fill a gap in the literature – namely, how does one conduct (or conduct oneself) in such an investigation, and what should one have in mind at various times?

It is published annually as a two-volume work and is also available online and in PDF format.

The volumes

This Guide is in two volumes. Volume I takes the reader through the issues and risks faced at every stage in the life cycle of a serious corporate investigation, from the discovery of a potential problem through its exploration (either by the company itself, a law firm or government officials) all the way to final resolution – be that in a regulatory proceeding, a criminal hearing, civil litigation, an employment tribunal, a trial in the court of public opinion or, just occasionally, inside the company's own four walls. As such, it uses the position in the two most active jurisdictions for investigations of corporate misfeasance – the United States and the United Kingdom – to illustrate the practices and thought processes of cutting-edge practitioners, on the basis that others can learn much from their approach, and there is a read-across to the position elsewhere.

Volume II takes a granular look at law, regulation, enforcement and best practice in the jurisdictions around the world with the most active corporate investigations spaces, highlighting, among other things, where they vary from the norm.

Online

The Guide is available at www.globalinvestigationsreview.com. Containing the most up-to-date versions of the chapters in Volume I, the website also allows visitors to quickly compare answers to questions in Volume II across all the jurisdictions covered.

The publisher would like to thank the editors for their exceptional energy, vision and intellectual rigour in devising and maintaining this work. Together we welcome any comments or suggestions from readers on how to improve it. Please write to us at:
insight@globalinvestigationsreview.com.

14

Forensic Accounting Skills

Glenn Pomerantz, Jared Crafton and John Thacher[1]

14.1 Introduction

This chapter aims to explain key concepts and leading practices in investigations from a forensic accounting perspective. It discusses the responsibilities and objectives of forensic accounting. It outlines the steps taken when conducting a forensic accounting investigation, including the identification, preservation and analysis of records. It addresses some of the challenges that arise when conducting investigations involving the dark web and cryptocurrency before discussing asset tracing and other methods of recovery.

The term 'forensic' means 'belonging to, used in, or suitable to courts of judicature or to public discussion and debate'.[2] Accordingly, forensic accounting involves the application of specialised knowledge and investigative skills and tools to matters in anticipation of possible litigation or dispute resolution, including in civil, regulatory, administrative and criminal enforcement matters.

Forensic accounting skills can be applied to a wide variety of investigations into alleged corporate and individual wrongdoing, including:

- misappropriation of assets;
- bribery and corruption;
- money laundering;
- financial reporting fraud;
- conflicts of interest; and
- non-compliance with policies and procedures, internal controls, laws, regulations or provisions of contracts.

---

1 Glenn Pomerantz is a partner, Jared Crafton is segment leader of technology and John Thacher is a managing director at BDO USA, PC.

2 Merriam-Webster, 'forensic' [online], www.merriam-webster.com/dictionary/forensic.

Forensic accounting objectives and responsibilities 14.2

Forensic accountants assist clients and triers of fact in determining:

- intent;
- the identity of parties that participated in a fraudulent scheme;
- the identity of parties that were aware of or should have been aware of the fraudulent scheme;
- how the scheme was perpetuated;
- why existing internal controls did not prevent or detect the scheme;
- quantum of the loss;
- potential avenues of recoveries; and
- strategies for remediation with the goal of future prevention and detection.

Forensic accounting responsibilities typically include:

- books and record review;
- forensic data analytics and artificial intelligence (AI);
- review of unstructured data, including emails and attachments (e-discovery or e-disclosure);
- corporate intelligence, including background checks;
- interviews;
- asset tracing;
- testimony; and
- design and implementation of remediation plans.

Identification and preservation of records 14.3

Forensic accounting investigations often begin with identifying the necessary steps to preserve data and relevant records. This may entail a litigation or litigation-like hold, preserving and restricting access to sensitive data, trade secrets, assets and communications. The allegations and preliminary fact pattern will dictate the specific records, data and assets that will be restricted or preserved, and to which employees and third parties will have their access limited.

See Chapters 33 and 34 on employee rights

Owing to the proliferation of electronic data, an increasingly important early step in many investigations is to determine what relevant information exists, its form (paper or electronic), its location (e.g., an on-site data centre, off-site at vendors or in the cloud), security measures in place over the data and the organisation's standard record retention and destruction policies and practices. The process of identifying, taking inventory of, organising, processing, hosting and producing relevant data that may be of use in an investigation or the resolution of a dispute is often referred to as e-discovery or e-disclosure. It is often necessary to collaborate with forensic technologists who can map IT systems and provide assistance with understanding the electronic records landscape. These technologists possess specialised methods for collecting this data in a defensible manner that is accepted by courts and regulators.

See Chapters 7 and 8 on beginning an internal investigation

14.4 Books and records review

The core function of a forensic accountant is the forensic analysis of internally generated books and records. The skills and experience necessary to conduct the forensic review are often rooted in a comprehensive accounting education, the training necessary for a Certified Public Accountant licence, Chartered Accountant designation or similar attainment, and experience in basic bookkeeping, which is surprisingly lacking in many forensic practitioners. Assessing the underlying bookkeeping of recorded transactions, often in conjunction with data analytics and account analysis, will allow the forensic accountant to:

- identify unusual entries;
- identify the initiator and approvers of unusual entries;
- determine how a scheme was disguised;
- identify overrides and bypasses of existing internal controls;
- prove the ill intent of a suspected fraudster; and
- help recover losses owing to fraud.

The act of making a false entry or failing to make an accounting entry at all is the type of trail a forensic accountant requires to document a potential fraud. Bookkeeping entries or lack thereof are the DNA of financial fraud. When this DNA is examined by the financial scientists (i.e., forensic accountants), financial frauds can be exposed and, in some instances, mitigated.

14.4.1 Analysis of financial records

Most books and records reviews begin with financial data from the organisation's accounting system. The accounting data can exist in several separate systems, such as:

- a general ledger, which is a master ledger that reflects all accounts and the sum of all accounting activity for the organisation;
- a general journal, where journal entries are initially recorded before being posted to the general ledger;
- books of original entry, which contain details of certain types of financial transactions, summaries of which are posted to the general ledger (e.g., books for sales, cash receipts, cash disbursements and payroll); and
- subsidiary ledgers and trial balances, which contain additional details of transactions and activities that appear only in summary form in the general ledger (e.g., accounts receivable and accounts payable ledgers).

The organisation's accounting is based on and documented by supporting records. These records form the crux of the forensic accountant's procedures for proving existence, validity and accuracy.

14.4.2 Review of supporting documents and records

Typically, within an investigation, the quantity of documents is narrowed to avoid overwhelming budgets and timelines. Culling this count via data

analytics, email review and a developed fact pattern will result in a focused collection of documents and relevant electronic records. Studying the processes and internal controls involved in the transaction cycle through these relevant documents will give the forensic accountant an understanding of the matter. For example, in a corruption investigation, several records may need to be reviewed, including:

- budgets;
- agent, distributor, supplier and customer contracts;
- bidding documents;
- margin data;
- price lists;
- market data;
- documentation for vendor set-up and vendor master file adds, moves and changes;
- sales by region, agent, territory and product;
- background checks;
- purchase order or purchase request;
- bill of lading or other confirmation of delivery and shipment and receipt of goods;
- proof of services;
- signed confirmation for services provided;
- invoice from a vendor or supplier;
- cheque or disbursement request form; and
- banking records.

These records might be reviewed for several reasons, such as:

- proving authenticity;
- establishing a timeline of events;
- testing their clerical accuracy;
- reviewing for inconsistencies, anomalies, trends and alignment with market rates and executed contracts;
- reviewing for agreement with accounting records;
- identifying the initiating and approving parties;
- reviewing for compliance with internal controls; and
- determining the authenticity of the document, the vendor and the services rendered.

Testing for authenticity of the record itself or of individual signatures on documents normally involves a highly specialised skill unless an anomaly is obvious. Accordingly, if an investigator suspects that a document on file is fraudulent or has been physically altered, or that a signature is not authentic, the document should be protected until someone with the necessary specialised

skills can assess its authenticity. Examples of obvious deficiencies in documentation include:

- inconsistencies in addresses, dates, page layout, and vendor invoice numbers and sequencing;
- lack of letterhead or other characteristics normally expected of a legitimate vendor;
- misspellings or other typographical errors; and
- variances with the vendor master file.

Some systems are hybrids of financial and non-financial information. Examples of these systems include the following:

- *Inventory*: In addition to cost information associated with purchases, the system may also provide data on quantities and dates of purchases, deliveries, shipments, inventory damaged or scrapped, and counts resulting from physical observation.
- *Payroll*: In addition to data on net amounts paid to employees, the payroll system will usually include other relevant data needed to calculate an employee's gross and net pay, including various worker classification codes, hours worked during a pay period, rates of pay, tax and withholding information, along with bank account information for the electronic transfer of funds to employees and home addresses.
- *Human resources*: In most large organisations, a human resources (HR) system that is separate from payroll is maintained. Included in this system are data on rates of pay and past pay increases, incentive payments and other financial data about each employee, as well as significant amounts of non-financial data, such as each employee's home address. HR information systems may also include vital information associated with an employee's initial hiring, such as background and reference checks, verification of information provided on an employment application, etc. This information can be important if the organisation anticipates filing an insurance claim to be indemnified for losses attributable to an employee.

Legal and data privacy considerations associated with each of these internal data sources vary from one jurisdiction to another, particularly with respect to payroll and personnel information. Domestic and foreign data privacy regulations must be considered before embarking on any use of such data in an investigation.

14.5 Forensic data analytics

Forensic data analytics refers to using a scientific method for the identification, collection, analysis and reporting of electronically stored information. This includes both structured data, such as financial records in a database, and unstructured data, such as files on a file server. The most commonly analysed data in forensic accounting investigations is financial, but several non-financial categories of data are also very useful to investigators. Each is explored below.

Data analytics generally has three applications in the investigative process:

- to initially detect fraud or non-compliance (e.g., monitoring performed by internal audit);
- to corroborate an allegation to justify launching an investigation (e.g., proving that an allegation received via a hotline appears to have merit); and
- to determine the extent of the wrongdoing.

Data analytics rarely proves that fraud or non-compliance occurred; rather, it identifies transactions or activities that have the characteristics of fraud or non-compliance so that they can be examined further. These are often referred to as anomalies in the data.

If an investigation ultimately leads to employee terminations or legal proceedings to recover losses, it is critical to have properly analysed the anomalies that data mining has identified. Could the anomaly, while often identified as a characteristic of fraud, also simply indicate a benign deviation? Failing to investigate and rule out non-fraudulent explanations for anomalies can have consequences that many investigators have learned about the hard way.

See Chapters 33 and 34 on employee rights

Identifying and exploring all realistically possible legitimate explanations for an anomaly is also called reverse proof. Examining and eventually ruling out all the valid possible legitimate explanations for an anomaly in the data or documentation can prove that the only remaining reasonable explanation is fraud or corruption.

Careful consideration of alternative theories for data and document anomalies is critical to protecting the organisation and the investigator from liability stemming from falsely accusing someone of wrongdoing.

Data mining to detect fraud or non-compliance 14.5.1

The nature of forensic data analysis can vary depending on which application or phase of the investigative process is involved. For example, as an initial detector of fraud or non-compliance through ongoing monitoring, forensic data analytics usually takes one of two broad, but opposite, approaches: identification of any activity that deviates from expectations, or identification of activity that possesses specific characteristics associated with problematic conduct.

The former approach is taken when acceptable behaviour is narrowly defined such that the slightest deviation warrants investigation. The latter approach is the more common one: it is driven by a risk assessment and is based on what fraud or non-compliance would look like in the data. For example, a shell company scheme might evidence itself by an address in the vendor master file matching an address in the employee master file. Any instances of such a match should be investigated.

In some cases, basing the decision of whether to investigate on a single characteristic in the data can result in numerous false positives. For this reason, more sophisticated data analytics often relies on the consideration of multiple characteristics in assessing the risk of activity being fraudulent or corrupt. These characteristics can be combined into a singular risk score per transaction that

can be aggregated by vendor, geography or other grouping. Risk scoring or risk ranking transactions can be useful for prioritising where to focus in the data.

Regardless of which of these two approaches is taken, data analytics often represents an essential tool for gathering evidence to lay the foundation for substantive examination of books, records and other evidence. Following the reverse-proof concept described above is critical once anomalies indicative of possible wrongdoing are uncovered.

14.5.2 Corroborating allegations

See Chapters 5 and 6 on whistleblowers

As a method of corroborating an allegation that has been received, data analytics can be of great value. It is a significant advantage to the investigator because, more often than not, it can be performed on electronic data without alerting the subject of the allegation. In this application, the allegation is first assessed in terms of what impact the alleged fraudulent or corrupt act would have on financial or non-financial data. It is important to understand how data flows through the organisation (e.g., how an invoice will flow from a business unit to finance and back to the business unit). The data can change quite a bit throughout different business processes, and this will need to be understood for a robust analysis to take place.

To illustrate, take the example of an allegation that workers in the shipping department of a warehouse are stealing inventory by short shipping orders to customers. Numerous sources of data, both financial and non-financial, could be analysed to assess the validity of this allegation:

- *gross profit margins*: an unexplained decline in gross profit margins by product or location (as a result of having to reship additional items with no associated revenue to satisfy the customer);
- *inventory purchases*: unexplained increases in purchases of certain inventory items without a corresponding increase in sales;
- *customer complaints*: customer service data indicating complaints about incomplete shipments, especially if those complaints can be correlated back to specific orders; and
- *shipping records*: using the customer complaint data, orders are correlated to specific shipments and employee names associated with filling and shipping these orders. Shipping records might also reveal more shipments to a customer than orders, indicating a second shipment was needed to complete the order after the customer complained.

This is a simple example, but one that illustrates that for every allegation, there likely exists data associated with either the perpetration or concealment of the fraud or non-compliance. This data normally exhibits one or more anomalies in comparison with data from similar transactions that do not involve fraud or non-compliance.

Using data analytics in an investigation 14.5.3

The final example of the application of forensic data analytics is during the investigation itself. Once an anomaly has been found to involve fraud or non-compliance, additional forensic data analysis and substantive forensic examination of the evidence may be performed to:

- determine for how long the activity has occurred;
- determine which accounts the fraud impacted;
- determine which employees (or third parties) participated in the fraud (i.e., assessing whether collusion was involved);
- quantify the financial damage resulting from the activity;
- identify other fraudulent or corrupt conduct by the same individuals; and
- determine how the fraudulent or corrupt act was concealed and how internal controls were circumvented.

Determining who is involved in the fraud as well as who possessed knowledge of it is critical to the mitigation and control enhancement objectives. According to a 2022 report by the Association of Certified Fraud Examiners (ACFE), nearly 58 per cent of all fraud and corruption schemes investigated involved multiple perpetrators.[3] Typically, losses tend to increase with multiple perpetrators, particularly when three or more individuals conspire to commit fraud. This figure has been steadily rising since the ACFE began studying fraud. The 58 per cent includes cases involving multiple internal perpetrators and those involving collusion between insiders and outsiders, such as vendors or customers.

The ACFE report indicates that 35 per cent of occurrences of fraud (especially with respect to asset misappropriations) are perpetrated through multiple methods. The allegation or investigation may have initially focused on only one specific method. Exploring other activities in which the subject might have the capability of engaging is an integral element of the investigation. Investigators and victims attempt to 'put a fence around the fraud' as early in the investigative process as possible. Understanding the responsibilities of the subject and the potential for unrelated schemes is essential for erecting the fence. Victims often desire a narrow investigative scope – a sort of wishful thinking. An investigator's worst-case scenario is missing a scheme perpetrated by a subject despite investigating the subject.

The question of who knew what and when can be particularly important in satisfying auditors in the context of financial reporting fraud. In addition to quantifying the financial statement impact from fraud, auditors rely on representations from management. Knowledge of whether previous representations came from fraudsters and the auditor's assessment of management's integrity are often important aspects of financial reporting fraud investigations.

3 Occupational Fraud 2022: A Report to the Nations, Association of Certified Fraud Examiners, https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf.

In the next sections, the distinction between financial and non-financial data is explored, followed by a discussion of internal versus external data.

14.6 Analysis of non-financial records

Increasingly, non-financial data is being analysed as a standard element of an investigation. Non-financial data can be classified into two broad categories: structured and unstructured.

Structured non-financial data is found in many systems, including those that include financial data mentioned above. Other systems, however, are entirely non-financial, but provide data that can be important to an investigation. Examples of non-financial systems commonly used for investigative purposes include the following:

- *Building security*: Many organisations now use tools that leave an electronic trail of the exact times and dates when specific employees entered or left the building. Records of visits by vendors and other visitors may be included in this system or be kept separately. Security information can be very useful in establishing timelines or the whereabouts of specific individuals.
- *Network data*: Much like accessing a building, networks maintain electronic records each time an authorised user logs on or off the system and may retain a record of various aspects of the user's network activity, such as which folders were accessed, which data was downloaded and which systems were used.
- *Call logs:* These can provide concrete evidence of business relationships or insights providing leads or further questions.
- *Customer service*: Data collected in the customer service system can have numerous applications in an investigative setting. Customer complaints about items missing from their orders, for instance, may indicate theft in the warehouse.

Unstructured data refers to data that does not readily conform to a database or spreadsheet format. Text associated with messages in emails, explanations for journal entries and other communications are the most common. Unstructured data also includes photographic images, videos and audio files.

See Chapters 33 and 34 on employee rights

Emails and text messages of interest to an investigator may involve messages within the organisation between employees and communications between organisation employees and vendors, customers or other third parties.

Similar to other electronic data, when a user 'deletes' this information, a backup or archive version is often left behind and is available to an investigator. Understanding an organisation's backup, archiving and storage practices is crucial to this part of an investigation.

Careful review of email, instant messaging or text message chains (and, if available, recordings of telephone calls) is crucial to most investigations and can provide an investigator with vital clues, such as:

- the timeline of events;
- the level of knowledge of events that specific individuals may have had;

- the extent of collusion among individuals;
- whether a subject or witness deleted email evidence;
- how the scheme was perpetrated; and
- whether there are indications of intent.

Establishing a timeline can be one of the most important requirements of an investigation. A complete timeline of events can often be established by integrating the separate timelines learned from a review of:

- systems and facilities access records;
- electronic transaction information (e.g., entries and approvals);
- electronic calendars of subjects-custodians;
- documentation (e.g., invoices and shipping records); and
- electronic communications, including metadata (e.g., emails, texts and instant messaging).

Email review is of particular importance in establishing intent. Intent, particularly in a civil lawsuit, may be inferred from communications that indicate an awareness that planned transactions or activities are in conflict with established policies and procedures or treatment of similar transactions. Although a rich source of behavioural history, email can quickly become overwhelming from a volume standpoint.

New techniques for document review 14.6.1

Over the past 20 years, data volumes have steadily doubled every 18 months, and this trend shows no signs of slowing down: the problem of overwhelming review volumes is here to stay. Fortunately, AI and assisted learning have been used steadily in e-discovery, with increasingly strong judicial support, since at least 2010. Within e-discovery, assisted learning has become an integral and well-established process with standardised and readily accepted statistical controls that allow practitioners to sift through large volumes of unstructured data while under tight timelines.

Assisted learning involves leveraging machine learning algorithms to optimise the review process by prioritising relevant documents for human review. As the algorithm continually updates and re-ranks the entire review population for probability of relevance, it leverages the decisions that human reviewers are making about documents. The technology is simply ranking documents based on their probability of being relevant and moves the highest ranked documents to the front of the review queue in a process known as prioritised review. This constant reshuffling of the deck allows investigators to focus their time on the documents that have the best chance of bringing real insights to their case.

Assisted learning offers multiple benefits. Enhancements in the efficiencies related to email review cost savings are significant and derive from reviewing only a small portion of the whole review population. An earlier, more comprehensive understanding of the investigation's scope and scale improves

the ability to manage both the investigation and expectations regarding timelines. This extremely adaptable approach also provides demonstrably higher levels of consistency, accuracy and defensibility in the review process. As new avenues for investigation come to the fore, searches used in conjunction with machine learning can help the algorithm prioritise different issues for review. Over the course of the investigation, assisted learning can continue to leverage the evolving understanding of the matter to serve up additional highly ranked documents.

There are many other modern techniques for prioritising and culling this type of unstructured information. Sentiment analysis, another form of AI, can assist with identifying the writer's emotional state. Additional forms of AI, typically referred to as natural language processing (NLP), can help correct for potential biases that investigators naturally bring to their review. For example, an investigator may select a list of search terms to run against email data to reduce the population for further review and bring the most important messages to the forefront. By creating these search terms, the investigator has leveraged what they know about the case, and this injects a natural bias.

By using AI, NLP, predictive analytics and machine learning, coupled with limited manual set-up, analysis and review, the data is allowed to speak for itself, and computer algorithms will cluster statistically relevant information. Typically, a combination of search terms and NLP is used. These types of analyses can identify pressures or rationalisations associated with fraudulent or corrupt behaviour. For example, an employee stating in communications that he or she feels unfairly treated or feels resentment towards management might be expressing a rationalisation for stealing from an organisation.

One potential pitfall of which investigators must be cognisant is ephemeral communications, which are communications that are temporary. There has been a proliferation of commercially available platforms that enable users to send messages that are deleted after a set period and are not recoverable. Most regulators have released guidance against companies utilising these platforms, but they are often seen on users' personal devices. Despite the messages themselves usually not being recoverable, evidence of the use of an ephemeral messaging platform can be part of a fact pattern when developing a case.

14.7 Use of external data in an investigation – corporate intelligence

Most data and documentation used in an investigation is internally generated: it comes from within the organisation or, in the case of invoices from a vendor, is otherwise readily available within the organisation. Occasionally, however, data or documentation that is only available from external sources often becomes essential in a forensic accounting investigation. External sources of data fall into two broad categories: public and non-public.

Public data and documents are those that are usually available to the general public either by visiting a website or facility or on request from the holder of the records. In many instances, public records are maintained by government

agencies. Examples of public records vary significantly from one jurisdiction to another, but some that may be useful to investigators are:

- business registrations, articles of incorporation and certain filings made by organisations;
- records of ownership or transfers of ownership of property (e.g., sales of land and buildings);
- criminal convictions of individuals and organisations, and certain other court records; and
- licences and permits issued by government agencies to individuals or businesses.

Availability and the extent of these records can differ markedly as an investigator seeks information from different parts of the world.

Increasingly, public records may also include information that an individual voluntarily makes publicly available. For example, when an individual posts photos or makes statements on social media, this information might be readily available to any and all viewers. Once again, investigators should always use caution when accessing this information, especially if the information is only available to 'friends' or other contacts to whom the individual has granted special access, but when social media information is made fully available to the general public, it can provide a treasure trove of information about a subject, such as assets owned, past and present employers, business relationships, social relationships, family relationships, places the subject has visited and lifestyle.

Websites that do not require special password or other access privileges are another public source of information. For example, a company's website, or that of a trade association or other membership group with which a subject might be involved, could provide clues about the subject's relationships, travels and past.

Even information that is no longer on a website might still be available to an investigator. The Wayback Machine[4] is an archive of more than 841 billion past pages on the internet.[5] Simply typing the URL of a website into the Wayback Machine will produce an index by date of prior versions of that website that have been archived and are available for viewing. Accordingly, an investigator may be able to find useful information from past editions of websites long after the information has been deleted.

Non-public records are private and confidential. Holders of these records are under no obligation to produce these records unless they have provided their consent or they are compelled to do so as a result of a legal process, such as a court order or subpoena. Records such as the personal bank statements of individuals who may be the subject of an investigation fall into this category. Investigators normally do not have ready access to these records.

4 Wayback Machine, www.archive.org.

5 As at October 2023.

14.7.1 Investigations involving the dark web

Another challenging and practically untraceable medium adopted by cybercriminals is the dark web, a small section of the deep web (content on the internet that is not readily accessible or visible through search engines) designed so it cannot be accessed through standard web browsers.[6] Although it allows for anonymous private communications for legitimate reasons (e.g., protection of free speech), it also allows for the distribution of harmful information and purchase of illegal goods and services that law enforcement agencies have difficulty tracing. For example, once an organisation's network has been breached, the intruder may extract sensitive information such as customer data, logins and passwords, banking details, taxpayer identification and social security numbers, and credit card details, and then sell this confidential information anonymously on the dark web marketplace and forum websites to buyers across the world.

Dark web investigations therefore require specialised forensic investigative tools, such as a secure dark web browsing platform with network and malware protection (e.g., firewalls and virus scanning) and secured data storage that maintains a strong custody chain for digital evidence, backed by strict and auditable compliance controls. Such tools can be used to search and monitor dark web communications, capture cryptocurrency information (e.g., blockchain wallet addresses), and attempt to identify and locate cyber fraudsters while capturing and analysing digital evidence in a forensically sound manner.

There are no anti-money laundering or know-your-customer (KYC) controls on the dark web: most dark web sites are anonymous and difficult to attribute to an owner because these sites use a '.onion' domain suffix, which can only be accessed via a Tor (The Onion Router) browser. Website traffic is bounced through randomly selected Tor entry, relay and exit nodes using separate embedded layers of data encryption for each hop in the network circuit (hence the term 'onion'). In addition, perpetrators are increasingly using cryptocurrencies to conduct illicit financial transactions via the dark web while hiding their identities.

14.7.2 Challenges associated with cryptocurrency

Cryptocurrencies and other blockchain-based digital assets, such as non-fungible tokens, present unique challenges and new opportunities for investigators seeking to trace them and attempt their recovery. Emerging cryptocurrencies are easily accessible and are widely accepted to the degree that fraudsters can, with minimal effort and risk, rely on them to move funds for the same purpose fiat currencies have long been used to transfer and conceal the source, nature and ownership of illicit funds. The added advantages of cryptocurrencies not requiring physical contact or interaction with banks has made

6 In addition to the dark web as a means to hide tracks, we are seeing an increase in the use of ephemeral messaging applications, which allow users to hide communications and permanently delete messages.

them the payment method of choice for perpetrators of ransomware attacks and other schemes aimed directly at defrauding victims (e.g., internet-based advanced fee schemes). Forensic investigators must, therefore, still follow the money trail and will be doing so more often with cryptocurrencies.

However, there is another side to the coin, so to speak: while cryptocurrencies provide a degree of pseudonymity, especially those designed to provide enhanced privacy, they do not provide complete anonymity. On the contrary, cryptocurrencies by design create an immutable public blockchain record of transactions that investigators can exploit to follow the money to a certain extent, provided they have the right tools and training.

As new cryptocurrencies are continually developed on different blockchains, investigators must also learn to follow transfers across them because fraudsters are commonly using cross-chain transfers and multiple types of cryptocurrencies to move illicit funds. There are also decentralised mixing protocols, and decentralised finance (DeFi) platforms (e.g., exchanges) that can facilitate laundering of digital assets. This requires investigative blockchain data analysis tools to be continually adapted and advanced to enable cross-chain analysis and asset tracing when dealing with mixers and DeFi platforms.

Although the on-blockchain transactions in cryptocurrencies can be traced using public blockchain data, for digital asset tracing to be successful for asset recovery or prosecution purposes, investigators must be able to trace transactions beyond the blockchain to identify the counterparties and the ultimate beneficiaries. This requires identifying and pursuing additional information from virtual asset service providers (VASPs) such as cryptocurrency exchanges, hosted wallet platforms and financial institutions providing custodial services for cryptocurrencies – the on-ramps and off-ramps to blockchains. These entry and exit points for cryptocurrencies are essential to fraudsters because for cryptocurrencies to be most useful to the ultimate beneficiaries, the digital asset value needs to be converted to or from fiat currency or other tangible assets.

A key goal of blockchain data analysis, therefore, is to correlate known blockchain addresses for on-ramps and off-ramps with blockchain data on suspect transactions to develop leads as to where cryptocurrency funds were converted. If this were a legitimate or regulated VASP, KYC information may have been collected, and more traditional investigative steps could be followed, such as the use of subpoenas, search warrants, regulatory inquiry or examination, and witness interviews.

See Chapters 12 and 13 on witness interviews

A key challenge for cryptocurrency-related investigations is the existence of illicit, unlicensed peer-to-peer exchanges that offer a way to convert fiat currencies to and from cryptocurrencies and DeFi platforms, allowing the exchange of cryptocurrencies through unregulated entities that do not collect KYC information. There are also providers of cryptocurrency laundering services, known as 'mixers', and decentralised mixing protocols, which offer a way for money launderers to obfuscate the actual counterparties to a blockchain transaction by mixing the cryptocurrency value with large numbers of other blockchain transactions going through the mixer (or mixing protocol).

Even transactions flowing in and out of a legitimate exchange can become untraceable using public blockchain data alone (without cooperation from the exchange to obtain internal account data) owing to the sheer volume of transactions flowing through a large exchange.

In summary, investigating financial crimes involving cryptocurrency and digital asset tracing will require specialist blockchain analysis and intelligence tools and services to identify leads to follow beyond the public blockchain. This may be easier to do when dealing with cryptocurrency compared with fiat currency that is physically transferred, but it also presents new challenges. Understanding these challenges and how to identify potential sources of additional attribution data for cryptocurrency transactions is essential. This will continue to be a changing landscape for investigators given the continually evolving technology and expanding array of new forms of blockchain-based cryptocurrencies and emerging DeFi platforms that promise to offer an even greater variety of financial services based on blockchain technology.

14.8 Tracing assets and other methods of recovery

If the subject has misappropriated cash (via intercepting incoming funds intended for the organisation, stealing cash on hand or fraudulently transferring funds from the organisation in connection with a disbursement fraud), one goal for most investigations is to secure the return of the funds. To do so, the investigation team must determine what the subject did with the money. Other sources of recovery may include culpable outside parties, including but not limited to collusive vendors, customers, agents and family members. Coverage for employee dishonesty losses under insurance policies and fidelity bonds may also be possible.

If the subject misappropriates other assets, a similar question must be addressed – where are the assets? Often, the subject's goal is to convert stolen items to cash by selling them. In other cases, the stolen asset itself may be of use to the subject.

Depending on how assets were stolen, varying degrees of a trail might be left by the perpetrator, enabling the investigation team to forensically determine the flow of money after it has left the organisation. The trail may begin with the company's books and records; however, it is usually intentionally made opaque by fraudsters through money laundering techniques, such as layering, transfers to shell companies, nominee shareholders and the use of clandestine communication techniques, cryptocurrencies and tax havens where criminal law enforcement assistance may be less effective.

Many of the records necessary to fully trace assets are non-public. But investigators are sometimes surprised to learn that a subject has left a public trail of valuable clues regarding the disposition or location of illegally obtained funds or assets that can be identified through indirect techniques, such as social media and internet due diligence, interviews of people in the know, establishing connections to the fraudster's other assets in more vulnerable venues and through multinational cooperation of law enforcement agencies.

Conclusion 14.9

Fraud continually rates as a leading risk in most surveys of business leaders all over the world. Data analytics – including AI, crypto wallet tracing, automated journal entry review, real-time monitoring of transactions and sophisticated corporate intelligence techniques – all serve to deter, detect, prevent and mitigate fraud. The daily battle between forensic accountants and fraudsters continues but is complicated by geopolitical influences, globalisation and economic pressures and impacted by a remarkable level of investment on both sides of the fence. Forensic accountants will continue to fight the fight on behalf of organisations and victims.