Fraud Intelligence
Business intelligence | informa
www.counter-fraud.com

FEATURE › INVESTIGATION

Investigation dos and don'ts

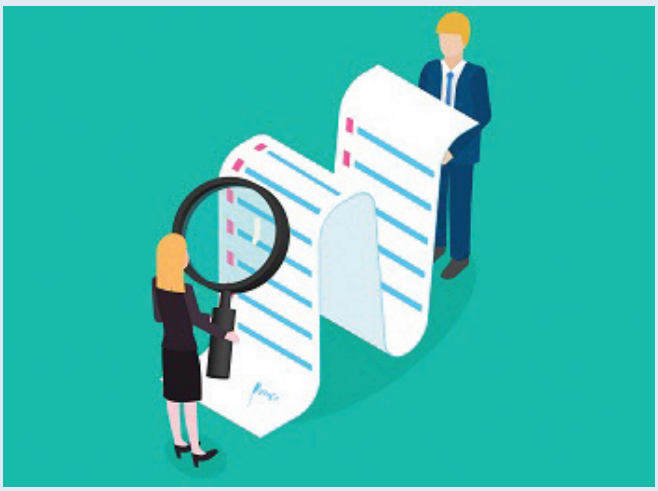
After receiving an allegation, the initial assessment of potential fraud or misconduct is crucial, says Cindy Hofmann of KPMG. She discusses how to deal with preliminary through to business continuity aspects, along with some useful tools.

Each year companies around the world lose billions of dollars because of white-collar crimes. Fraud, misconduct, corruption and similar violations of laws and regulations are the most common incidents. They can damage a company's reputation and undermine public trust in the market. Conducting an investigation based on a proven methodology helps to identify the perpetrators, quantify the damage, allocate responsibilities and even potentially recover assets. This article provides important guidance on how to proceed professionally if an allegation of this nature is received. The structure resembles the high-level chronology of an investigation – with relevant aspects that investigation practitioners should consider before, during and after the actual act of investigating.

Initial assessment

When the people in charge of an investigation receive an allegation of (potential) fraud or misconduct, a carefully conducted initial assessment is indispensable. Otherwise, a rushed and unstructured approach could lead to the loss of important evidence as well as confusion among stakeholders. Below are five preliminary questions you may want to consider as part of the initial assessment:

1. What are the suspicions based on?
Is the suspicion based on hard evidence (such as accounting documents, annual reports, emails, etc) or are there only rumours of potential misconduct? Is the information traceable and reliable? Which evidence would be available and where can you find it? The more conclusive the evidence, the more likely it will be possible to launch an investigation. Moreover, if evidence is easily assessible, investigation practitioners are better able to plan the next steps. However, evidence available across borders will mean complications. One needs, for example, to consider data protection laws and how and who is permitted to obtain the evidence in a forensically sound manner.



2. Who are the people or companies involved?
Who has expressed the suspicions and against whom? Are current or former employees, clients, suppliers or even competitors involved? How will the people react when the investigators confront them? At this point, you may need to consider that former employees no longer have an obligation to cooperate and they might not be reachable.

3. What is the potential damage?
What is the potential financial and/or reputational damage to the company? Depending on the size and nature of the possible damage, the company may decide to confine or broaden the investigation. Third party claims and impending legal disputes can be major determinants of the potential damage as well.

4. Has there been an infringement of the law?
Has there been an infringement of civil or criminal law or supervisory requirements? We tend to allocate more time and financial investment to an investigation when there has been an infringement of the law.

5. What immediate actions should I take?
Firstly, depending on the severity of the incident, it is helpful to involve the communications department: together you

should decide what you will communicate internally and externally. Secondly, when an incident occurs, it is very useful to have a fraud response plan in place in order to react quickly, efficiently and professionally. A fraud response plan defines, for example, who will be informed and who investigates the matter to ensure a seamless process. Thirdly, depending on the size of your investigation team and the severity of the incident, it may make sense to involve other (independent) experts to assist with the investigation. Once the investigation team is defined, further aspects such as required infrastructure need to be considered. Finally, but no less important for that, those in charge of an investigation have to decide if a dawn raid on the premises to obtain and secure evidence is necessary. If so, questions like when and how they will perform it, need to be addressed.

Securing evidence

Prior to commencing or at the start of an investigation, the aim is to secure evidence. In this context, it is especially important to maintain a chain of custody at all times. If the chain of custody is not maintained, it could mean the evidence obtained is not admissible in court. Due to the fact that it is never known at the start of an investigation whether the case will in fact go to court later on, each and every investigation should be conducted in such a manner that the evidence is admissible in court. We have seen cases where the opposing party attacks the collection and retention process to cast doubt on the integrity of evidence and render it inadmissible.

When securing evidence, data protection and data privacy are highly sensitive issues whether or not the investigation is cross-border. Regulations and policies might affect an investigation by restricting access to and use of private information gathered from company equipment.

Increasing digitalisation means one can gather more electronic evidence than before. However, depending on the organisation and from how far back in the past information is collected and stored, some evidence may only be physically available, such as certain contracts with counterparties in particular countries, or invoices or purchase orders. Anyway, one of the key challenges around electronic evidence is to identify and process relevant data (eg, from mobile devices, emails, scanned, deleted or encrypted data) in an efficient and goal-oriented way.

Gathering evidence during a dawn raid is a special case. There is the element of surprise but many things can go wrong, especially if you do not plan with care. Important factors, just to mention a few, are the team structure, security aspects, access to IT devices, documentation of the evidence, availability of the target person(s), ensuring continuation of the operating business and the proper storage of all the evidence gathered. We've seen instances where the playbook for a dawn raid has not been accurately and diligently prepared, resulting in small but impactful mishaps. It might be that the target person is absent or they are very aggressive but no security for other employees and investigators has been arranged. There may be no plan for how and when customers will be informed that their previous contact is no longer with the organisation or payments are delayed if the target person was the only one with access to the bank accounts.

Fraud and misconduct examination

Once the investigators have obtained relevant evidence, they need to decide how to explore it. Since there is often a lot of evidence, usually more than can be examined – it can be like the proverbial 'finding a needle in a haystack' – some of the following considerations may help in getting started:

Goals

Always set clear goals for the investigation upfront.

Hypotheses

Based on the allegation(s) received, consider and draft hypotheses to help target the fraud examination on specific areas and to set the scene to reach the goals.

Evaluation of evidence

After documenting the evidence obtained (as well as the chain of custody!) you should evaluate and sort the available evidence to determine the most relevant for review.

Internal/external evidence

You need especially to consider evidence that may be located externally (ie, with third parties, suppliers, business partners, group companies) as opposed to internal evidence.

Physical/electronic evidence

Consider which parts of physical documents you need to review to achieve the goals and prove the hypotheses, and potentially consider digitalising the physical documents to make review, storage and use of them more efficient.

Corporate intelligence on target persons/entities

Collect relevant information on your targets by researching their background, profile, adverse media etc, to help you fine-tune your hypotheses or find related parties who could be involved in the potential fraud scheme.

Interviews

Be sure to prepare interview questions well, take notes and consider letting the respondents sign these notes (this forms a better basis for evidence later on).

Technology in investigations

In order to review large amounts of data – such as emails, electronic documents, etc – more efficiently and in a more targeted way, investigators use various tools. Since a detailed description of the technology would go beyond the scope of this article, the focus here is on three specific methods.

Early Case Assessment (ECA)

You could, for example, use the software BrainSpace to understand the data better as well as to aid you in developing themes and issues during the initial stage of an investigation.

When used upfront it can help to draft the scope and criteria (ie, keywords, date range and custodians). By running searches for the related keywords, you can identify themes within the data that are relevant to the investigation and useful for fine-tuning the keywords and date ranges.

Visualisation dashboards

Using visualisation dashboards could assist in obtaining a high-level insight into the data, highlighting, for example, anomalies and encrypted or corrupt files. Applying visualisation could help you to see trends and outliers.

Technology Assisted Review (TAR)

TAR helps arrange documents so you can see the most relevant more quickly. Practical experience affirms its huge value.

Business continuity

Once the investigation is complete, it is important to ensure that business can continue as usual. Using proper communication channels, the company might need to inform its stakeholders internally as well as externally of more or less of the specific findings and lessons. In addition, it should raise the awareness of reporting channels if there are similar incidents. Key personnel may have to be replaced and management might have to reconsider access rights to bank accounts and/or certain accounting practices. This kind of situation will certainly prompt control improvements, gap analysis as well as extra employee training.

Undoubtedly, the investigation itself generates the most fuss; nonetheless, the initial assessment before and the business continuity aspects afterwards are equally important. In order to avoid (potential) financial and/or reputational damage, make sure that you deploy the right tools and an experienced team of investigators.

■ **Cindy Hofmann** (+41 58 249 56 25, cindyhofmann@kpmg.com) is a forensic specialist with KPMG in Zurich, Switzerland.

Fraud Intelligence is published by Informa Law, 13th Floor, 240 Blackfriars Road, London, SE1 8BF. *Fraud Intelligence* gives you practical insight, analysis and tools to combat fraud, whether you're in the corporate or non-commercial sector. Our financial crime content is available online via single-user subscriptions or multi-user licences at https://www.i-law.com/ilaw/financial.htm including *Lloyd's Law Reports: Financial Crime* (ISSN 1756 7637) and *Compliance Monitor* (ISSN 0953 9239).

Client Services: Please contact Client Services on tel: +44 (0)20 3377 3996; +65 6508 2430 (APAC Singapore), or email clientservices@i-law.com

Editorial queries: Please contact Timon Molloy on tel: +44 (0)20 7017 4214, or email timon.molloy@informa.com

Informa Law is an Informa business, one of the world's leading providers of specialist information and services for the academic, scientific, professional and commercial business communities.

Registered Office: 5 Howick Place, London SW1P 1WG. Registered in England and Wales No 1072954.

Print managed by: Paragon Customer Communications.