PLANNING AND CONDUCTING A FRAUD EXAMINATION

Fraud examinations represent perhaps the most important part of a fraud examiner's wide and varied body of knowledge. The term *fraud examination* refers to the process or methodology of resolving allegations of fraud from inception to disposition, as well as assisting in the prevention and detection of fraud. This includes activities such as conducting fraud investigations, performing fraud risk assessments, monitoring transactions and analyzing data for red flags of fraud, and evaluating anti-fraud policies and controls.

Many factors can impact a fraud examination, complicating the process for the fraud examiner and the investigation team. However, careful and thorough planning will mitigate these challenges and ensure that those involved are prepared to carry out a responsible and thorough engagement that achieves its goals without jeopardizing results. Taking the time to properly plan a fraud examination greatly increases its chance of success.

Why Conduct a Fraud Examination?

There are many reasons why organizations choose to conduct fraud examinations. In particular, a properly executed fraud examination can address numerous organizational objectives, including:

- Identifying improper conduct
- Identifying the persons responsible for improper conduct
- Stopping ongoing fraud
- Sending a message throughout the organization that fraud will not be tolerated
- Determining the extent of potential liabilities or losses that might exist
- Helping facilitate the recovery of losses
- Stopping future losses
- Mitigating other potential consequences
- Strengthening internal control weaknesses

In some instances, a fraud examination might be required by law. A duty to investigate can arise from statutes, regulations, contracts, or common law duties. For example, a corporation's directors and officers owe a common law duty of care to their organization and shareholders; therefore, when suspicions of fraud arise, it might be necessary for them to commission an investigation to ensure that they have full knowledge of such issues affecting the company.

Likewise, some laws hold employers accountable for investigating employee complaints involving certain matters, such as retaliation, discrimination, harassment, and similar issues.

What Fraud Examination Entails

The fraud examination process encompasses a variety of tasks that might include:

- Obtaining evidence
- Reporting
- Testifying to findings
- Assisting in fraud detection and prevention

Obtaining Evidence

The value of a fraud examination rests on the credibility of the evidence obtained. Evidence of fraud usually takes the form of documents or statements by witnesses; therefore, fraud examiners must know how to obtain documentary evidence and witness statements properly and legally.

Reporting

Once the fraud examiner has obtained and analyzed the evidence, they must report their findings to the designated individuals (e.g., management, the board, or the audit committee). A *fraud examination report* is a narration of the fraud examiner's specific activities, findings, and, if appropriate, recommendations.

Such communications are necessary so that management can evaluate the evidence and determine the appropriate course of action.

The results of an examination can be communicated in various ways. The appropriate method of communication depends on the facts at issue and the audience, but most reports are communicated orally, in writing, or both.

When communicating the results of a fraud examination, the fraud examiner is responsible for providing clear, accurate, and unbiased reports reflecting the fraud examination results. This need arises from the possibility that such results might be read or used by various groups of people, such as organization insiders, attorneys, defendants, plaintiffs, witnesses, juries, judges, and the media.

Testifying to Findings

Often, fraud examiners are called upon to provide testimony and report their findings at a deposition, trial, or other legal proceeding. When providing testimony, fraud examiners must be truthful regarding their investigation process and findings. They should also communicate in a clear and concise manner.

Assisting in Fraud Detection and Prevention

Fraud examiners are not solely responsible for the prevention of fraud. Such responsibilities typically belong to management or other appropriate authorities. Nevertheless, fraud examiners are generally expected to actively pursue and recommend appropriate policies and procedures to detect and prevent fraud, especially when their examinations identify issues with anti-fraud controls.

Because of their education, experience, and training, CFEs are uniquely qualified to assist organizations in the prevention and detection of fraud.

Fraud Examination and Forensic Accounting

Although fraud examination shares certain characteristics with forensic accounting, it is a different discipline.

Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation. The word *forensic* is defined by Merriam-Webster.com as "used in, or suitable to courts of judicature or to public discussion or debate." Therefore, *forensic accounting* is litigation support involving accounting evidence or information.

Accordingly, many fraud examinations can be considered forensic accounting, but not all forensic accounting is fraud examination. For example, an individual hired to appraise property in a minority shareholder derivative suit would engage in forensic accounting even if the engagement does not involve fraud.

Although both accountants and non-accountants can conduct fraud examinations, only accountants can perform forensic accounting work. In addition, while forensic accounting is litigation support work that involves accounting evidence or information, fraud examinations only involve anti-fraud matters and do not require accounting evidence or information.

Forensic accounting can include many professional services. Typically, forensic accountants perform assignments involving:

- Bankruptcies, insolvencies, and reorganizations
- Workplace fraud investigations
- Calculations of economic losses
- Business valuations
- Professional negligence

Fraud Examination Methodology

Again, fraud examination is the methodology of resolving signs or allegations of fraud from inception to disposition. The fraud examination methodology establishes a suggested uniform and legal process for resolving signs or allegations of fraud in a timely manner. It provides that fraud examinations should move in a linear order, from the general to the specific, gradually focusing on the perpetrator through an analysis of evidence.

Fraud examinations involve efforts to resolve allegations or signs of fraud when the full facts are unknown or unclear; therefore, fraud examinations seek to obtain facts and evidence to help establish what happened, identify the responsible party, and provide recommendations where applicable.

When conducting a fraud examination, the fraud examiner should do the following:

- Assume litigation will follow.
- Act on predication.
- Approach investigations from two perspectives.
- Begin with the general before moving to the specific.
- Use the fraud theory approach.

Assume Litigation Will Follow

Each fraud examination should be conducted with the assumption that the case will result in legal proceedings. This will ensure that the fraud examiner maintains compliance with the proper rules of evidence and remains well within the guidelines established by the legal systems.

Since documents make up so much of the evidence in fraud cases, it is important to anticipate motions challenging the admissibility of evidence and to understand the appropriate way of

collecting and handling evidence so that it will later be accepted by a court. Collection practices are especially important for electronic data, which is more volatile than tangible sources of information.

Act on Predication

Fraud examinations must adhere to the law; therefore, fraud examiners should not conduct or continue fraud examinations without proper predication. *Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe that a fraud has occurred, is occurring, or will occur. In other words, predication is the basis upon which a fraud examination, and each step taken during the examination, is commenced.

A fraud examiner acts on predication when there is a sufficient basis and legitimate reason to take each step in an examination.

Accordingly, fraud examiners should begin a fraud examination only when there are circumstances that suggest fraud has occurred, is occurring, or will occur, and they should not investigate beyond the available predication. If fraud examiners cannot articulate a factual basis or good reason for an investigative step, they should not do it. As a fraud examination progresses and new information emerges, fraud examiners should continually re-evaluate whether there is adequate predication to take each additional step in the examination.

If fraud examiners act without predication, they might expose themselves and their clients or employers to liability.

The requirement for predication, however, does not bar fraud examiners from accepting other forms of engagements in circumstances where predication is lacking. For example, if employees appear to be living beyond their means (i.e., living a more extravagant lifestyle than their income would seem to allow), there could be many reasons other than fraud to explain the disparity, such as an inheritance, a higher-earning spouse, or royalties received from mineral rights. In such circumstances, a fraud examiner can conduct a fraud risk assessment for consulting purposes even if there is not necessarily reason to believe a fraud has occurred, is occurring, or will occur.

Approach Investigations from Two Perspectives

Fraud examiners should approach investigations from two perspectives: (1) by seeking to identify evidence that supports that fraud *has* occurred and (2) by seeking to identify evidence that supports that fraud *has not* occurred. The reasoning behind this two-perspective approach is that both sides of fraud must be examined because *proof of fraud must preclude any explanation other than guilt* in most legal systems. Additionally, approaching fraud examinations from two perspectives preserves the fraud examiner's objectivity and helps ensure that bias does not influence an examination's results.

Begin with the General Before Moving to the Specific

Fraud examinations commence when the full facts are unknown or unclear; therefore, fraud examinations should begin with general information that is known and then transition to details that are more specific as more information is obtained.

For example, consider the order of interviews in fraud examinations. In most examinations, fraud examiners should start interviewing people who are less involved in the issues related to the examination before interviewing witnesses who appear to be more involved. Thus, the usual order of interviews is as follows:

- Neutral third-party witnesses, starting with the least knowledgeable and moving to those who are more knowledgeable about the matters at issue
- Parties suspected of complicity, starting with the least culpable and moving to the most culpable
- The primary suspect(s) of the examination

Use the Fraud Theory Approach

When conducting fraud examinations, fraud examiners should follow the fraud theory approach. The *fraud theory approach* is an investigative framework designed to help fraud examiners organize and direct examinations based on the information available at the time. It is a variation of the traditional scientific method often applied to hard science investigations.

The fraud theory approach provides that, when conducting investigations into allegations or signs of fraud, fraud examiners should make a hypothesis (or theory) of what might have occurred based on the known facts. Once fraud examiners have created a hypothesis, they should test it through the acquisition of new information (or correcting and integrating known information) to determine whether the hypothesis is supported. If, after testing a

hypothesis, fraud examiners determine that it is not supported, they should continually revise and test their theory based on the known facts until it is supported; they conclude that no fraud is present; or they find that the fraud cannot be proven.

Simply put, the fraud theory approach involves the following steps:

- Analyzing available data
- Creating a hypothesis
- Testing the hypothesis
- Refining and amending the hypothesis

The following internal fraud case study illustrates the concepts involved in the fraud examination process. Although the case study is based on an actual incident, the names and certain other facts have been changed for privacy considerations.

LINDA REED COLLINS CASE STUDY

Linda Reed Collins is the purchasing manager for Bailey Books Incorporated in St. Augustine, Florida. Bailey, with $226 million in annual sales, is one of the country's leading producers of textbooks for the college and university market, as well as technical manuals for the medical and dental professions.

Bailey's headquarters consists of 126 employees, plus numerous sales personnel in the field. Because of the competitive nature of the textbook business, the company's profit margins are quite thin. Bailey's purchases average about $75 million annually, consisting mostly of paper stock and covering used in the manufacturing process. The great majority of the manufacturing is done in Mexico through contracts with the Mexican government.

The purchasing function is principally handled by three purchasing agents. Linda Reed Collins is the purchasing manager and has two other buyers who report to her, plus another 18 clerical and support personnel.

Because Bailey Books is required by investors and lenders to have audited annual financial statements, Bailey employs a large regional certified public accountant (CPA) firm to conduct its annual audit and also has a staff of five internal auditors.

All internal fraud matters within Bailey are referred to Loren D. Bridges, a CFE. Often, internal fraud issues at Bailey involve skimming by Bailey's cashiers, but Bridges also receives a constant stream of complaints alleging misconduct by Bailey Books' salespeople and distributors.

On January 28, Bridges received a telephone call in which the caller wanted to keep his identity hidden. The caller claimed to have been a "long-term" supplier of books, sundries, and magazines to Bailey. The caller said that ever since Linda Reed Collins took over as purchasing manager for Bailey several years ago, he has been systematically forced out of doing business with Bailey. Although Bridges queried the caller for additional information, the caller hung up the telephone.

Under the facts in this case study, there could be many legitimate reasons why a supplier to Bailey would feel unfairly treated. Linda Reed Collins could be engaged in fraud, as the caller claimed, or the caller could be someone who has a personal vendetta against Collins and wants to get her dismissed. That is, Bridges does not have enough information to know if the caller was forced out of doing business with Bailey or why this might have been the case. Because Bridges does not have all the facts, he should investigate the matter using the fraud theory approach.

Analyzing Available Data

Under the fraud theory approach, Bridges should begin by analyzing the available data so he can create a preliminary hypothesis of what has occurred. The tip provides the original information.

If those responsible determine that an audit of the entire purchasing function is warranted to gather additional data, the audit would be conducted at the time this determination is made. When conducting the audit, the internal auditors should keep in mind that there is a possibility that fraud might exist.

Creating a Hypothesis

Once Bridges has analyzed the available data, he should create a preliminary hypothesis of what has occurred. The hypothesis should be a worst-case scenario. That is, based on the caller's statements, Bridges should determine the worst possible outcome. Under these facts, the worst possible outcome would be that one of Bailey's purchasing agents has been

accepting kickbacks to direct business to a particular vendor, therefore diverting business away from the person who reported the tip.

Fraud examiners can create hypotheses for any specific fraud allegation (e.g., a bribery or kickback scheme, embezzlement, conflict of interest, or financial statement fraud).

Testing the Hypothesis

Once Bridges has created a hypothesis, he should test it through the acquisition of new information or by correcting and integrating known information.

Testing a hypothesis involves creating a speculative scenario. For example, in the Linda Reed Collins case study, Bridges hypothesizes that a vendor is bribing a purchasing agent to receive more business that previously went to other vendors. He would test this hypothesis by looking for some or all of the following facts:

- A vendor who is receiving an unusually large amount of business
- Purchases of high-priced, low-quality goods or services over an extended period
- A purchasing agent who has a personal relationship with a vendor
- A purchasing agent with the ability to direct business toward a favored vendor
- A purchasing agent's lifestyle that suggests unexplained wealth or outside income

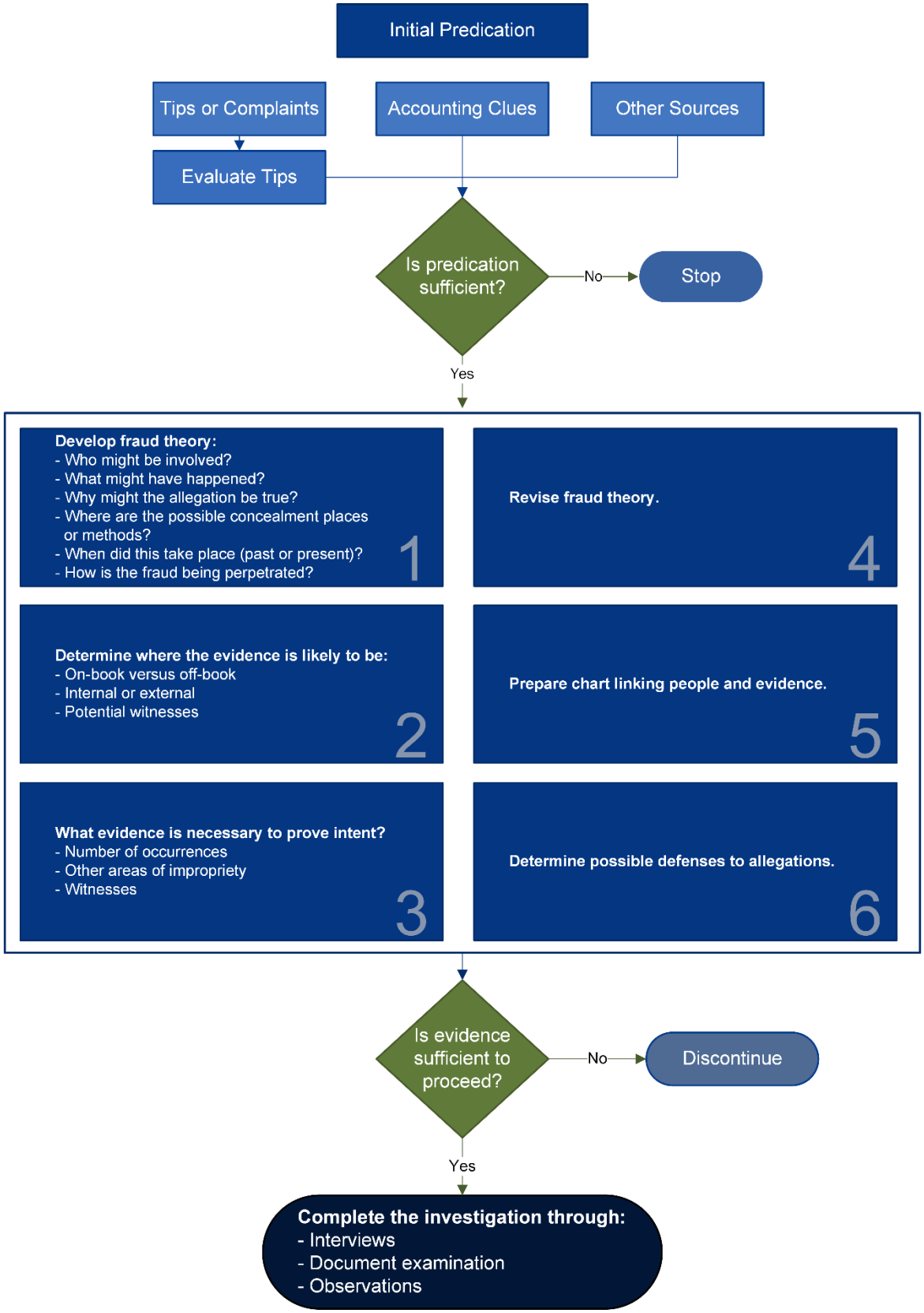
Bridges could readily look for facts indicating a bribery scheme or establish whether a vendor is receiving an unreasonably large proportion of Bailey Books' business when compared to similar vendors. Bridges could ascertain whether Bailey Books was paying too much for a particular product, such as paper, by simply calling other vendors and determining competitive pricing. He could also determine whether a vendor has a personal relationship with a purchasing agent by discreet observation or inquiry, public records searches, and social media research. Additionally, Bridges could ascertain whether a particular purchasing agent had the ability to direct business toward a favored vendor by determining who is involved in the decision-making process. He could learn about the agent's lifestyle by examining public documents such as real estate records and vehicle titles, examining the agent's social media accounts, and conducting discreet inquiries with other employees.

Refining and Amending the Hypothesis

If, after testing a hypothesis, the fraud examiner determines that it is not supported by the evidence, the fraud examiner should continually revise and test the hypothesis based on the known facts. The fraud examiner should also consider other ways of developing evidence.

For example, if Bridges tests his hypothesis that a vendor is bribing a purchasing agent of Bailey Books and learns that the facts do not fit the presence of a bribery scheme, he should revise his hypothesis and retest it. It should be noted that if a fraud examiner finds that the evidence does not support a bribery scheme, it could be that no fraud is present *or* that the fraud was not committed using bribery. More hypotheses should be developed and tested to rule out other methods of committing fraud.

The following flowchart sets forth how the fraud examination process is used to investigate signs or allegations of fraud.


Initial Predication
Tips or Complaints
Accounting Clues
Other Sources
Evaluate Tips
Is predication sufficient?
No
Stop
Yes
Develop fraud theory:
- Who might be involved?
- What might have happened?
- Why might the allegation be true?
- Where are the possible concealment places or methods?
- When did this take place (past or present)?
- How is the fraud being perpetrated?
1
Revise fraud theory.
4
Determine where the evidence is likely to be:
- On-book versus off-book
- Internal or external
- Potential witnesses
2
Prepare chart linking people and evidence.
5
What evidence is necessary to prove intent?
- Number of occurrences
- Other areas of impropriety
- Witnesses
3
Determine possible defenses to allegations.
6
Is evidence sufficient to proceed?
No
Discontinue
Yes
Complete the investigation through:
- Interviews
- Document examination
- Observations

Develop a Fraud Response Plan

When evidence of misconduct arises, management must respond in an appropriate and timely manner. During the initial response, time is critical. To help ensure that an organization responds to suspicious fraud-related activity efficiently and effectively, management should have a response plan in place.

A *fraud response plan* details the actions that members of an organization will take when suspicions of fraud arise. Therefore, it must be created *before* cases are reported to guide the initial response to accusations. Because every fraud is different, the response plan should not specify how all fraud examinations should be conducted. Instead, it should help organizations manage their responses and create environments that minimize risk and maximize the potential for success.

Additionally, a response plan allows management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner. Having a response plan in place sends a message that management takes fraud seriously.

More specifically, the fraud response plan should guide the necessary action when potential fraud is reported or identified.

A response plan should not be unduly complicated. For a response plan to work in high-pressure and time-sensitive situations, it must be simple to understand and apply.

While the appropriate response will vary based on the event, management should include a range of scenarios in the response plan, taking into consideration previous frauds within the organization and fraud risks specific to the industry or business sector in which it operates.

Organizations without a fraud response plan might not be able to respond to issues properly and will likely expend more resources and suffer greater harm than those that have such a plan in place. Conversely, having a response plan puts an organization in the best position to respond promptly and effectively.

This section explores the elements of a fraud response plan, which include:

- Reporting protocols
- A response team
- Factors used to determine the course of action

- Litigation hold procedures
- Principles for documenting the investigation
- A fraud incident report log

Reporting Protocols

One of the first steps when developing a response plan is to establish reporting protocols for tips, allegations, and other indicators of improper activity. Reporting protocols are necessary to ensure that designated individuals are notified immediately to enable a prompt response.

Reporting protocols should outline notification principles and escalation triggers, depending on the nature and severity of the allegations. That is, they should indicate how to communicate the incidents to the appropriate level of management. For example, a fraud response plan might instruct employees to report suspicions of fraud to their manager (if possible), a designated human resources (HR) or compliance officer, or the head of audit and enforcement.

Next, the issue should be reported to the party or parties responsible for conducting an initial assessment to determine how to respond and whether a full investigation is necessary.

Additionally, organizations should provide multiple channels for reporting concerns about fraud, including a whistleblower program that allows for anonymous reporting where possible, and should at least implement a whistleblower protection policy.

A Response Team

No single person can effectively address every fraud-related issue. Therefore, the fraud response plan must identify key individuals who might be required to respond to a particular fraud. The response team members will vary depending on the facts and the potential severity of the suspected fraud, but the team might include:

- Legal counsel
- A representative of management
- A CFE
- The finance director
- A representative of internal audit
- Audit committee members
- A C-level executive

- IT personnel
- An HR representative
- Security personnel

Factors Used to Determine the Course of Action

Again, the response team should determine the appropriate course of action when fraud is suspected. In general, if an allegation of fraud-related misconduct arises, management should conduct an investigation, but there are other alternative actions it might decide to take. As part of the fraud response plan, management should identify a list of factors it will use to make this decision. Identifying such factors will help the response team determine whether to escalate an incident into an investigation.

Each organization will have different criteria for deciding whether allegations or suspicions qualify for a formal investigation, but common considerations include:

- Credibility of the allegation
- Type of incident
- The subject of the allegation
- The business purpose of the activity at issue
- Seriousness or severity of the allegation
- Potential negative impact
- Likelihood that the incident will end up in court
- The ways in which similar incidents were handled in the past

Litigation Hold Procedures

If an organization does not already have litigation hold procedures in place following a credible allegation of fraud, management should institute them immediately. A *litigation hold* refers to the steps an organization takes to notify employees to suspend the destruction of potentially relevant records when the need to preserve information arises.

Litigation hold procedures are necessary to ensure that potentially responsive documents are not destroyed once allegations of misconduct arise. The failure to preserve relevant evidence could have several adverse consequences, including the government's questioning of the integrity of any fraud investigation, monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defenses.

To establish litigation hold procedures, management should:

- Identify the scope of litigation hold procedures (i.e., the locations that the litigation hold procedures will cover).
- Examine how information moves through the organization.
- Determine how to identify relevant documents.
- Develop a process to ensure such information is preserved.

Litigation hold procedures should apply to individual communications (e.g., email, chat messages, voice recordings), data on shared devices (e.g., network folders, cloud storage accounts), system backup files, and archived data.

In general, litigation hold procedures should be developed so the organization can:

- Promptly notify employees who might possess relevant documents.
- Issue a preliminary hold order to all individuals and employees who might possess relevant information.
- Promptly notify IT personnel and get their involvement if electronic data is at issue.
- Notify employees and IT personnel of their duty to preserve.
- Suspend any deletion protocols.
- Prohibit the destruction, loss, or alteration of any potentially relevant documents.
- Prohibit employees from destroying, hiding, or manipulating documents.
- Alert employees regarding the risk to the company and its employees if they fail to heed the litigation hold request.

Moreover, establishing litigation hold procedures will help those involved in an investigation identify the relevant sources of information quickly, and it will help them understand the technology options available for searching, analyzing, and reviewing data.

Even though litigation holds should apply to both electronic data and physical documents, electronic data contains certain attributes that make executing a timely litigation hold more difficult. Specifically, electronic data might only be available for a temporary period, as business practices are often designed to free up storage space by deleting this type of information. Electronic data can reside in numerous locations and identifying relevant electronic data within today's large and complex data systems can be challenging and costly. A key objective of a litigation hold is to suspend any automatic document deletion programs or rules that might be in place.

If an organization operates internationally, it is more difficult to execute a timely hold. In such cases, management should consider retaining an outside expert to help with the data search and preservation.

Principles for Documenting the Investigation

Management should establish principles in the response plan for documenting information during each phase of a fraud investigation. The principles should be designed to record all information relevant to or created during each phase of a fraud investigation, including the initial response, that is used to support decision-making.

A Fraud Incident Report Log

Management should also develop a fraud incident report log of all suspicions of fraud, including those not investigated, to serve as a record of the organization's response efforts. Once a suspicion of fraud arises, the issue should be recorded and detailed in the log, and as the issue progresses, the log should be modified. Ultimately, it should contain details of actions taken and conclusions reached.

The report log should include information on the following items:

- How the organization became aware of the suspected fraud, including the name of any complaining party, if available
- The date the issue was raised or reported
- The nature of the suspected fraud
- Department or divisions involved
- Suspect employees or parties
- Actions taken

Refer to Appendix C in this section of the *Fraud Examiners Manual* for a sample fraud incident report log.

Initial Response to Suspicions or Allegations of Fraud

When responding to suspected and detected incidents of fraud, time is critical. Management and fraud examiners must be prepared to address a number of issues in a short amount of time, sometimes under stressful conditions.

This section explores the first steps that management and fraud examiners should take when a fraud-related incident becomes known, and it provides a list of tips for managing and organizing the process of responding to suspected and detected incidents of fraud.

As a reminder, when a suspicion or allegation of fraud arises, management must respond quickly. Failure to do so could result in legal proceedings, enhanced penalties, and enforcement actions by government regulators.

Fraud can be discovered in several ways, including via a tip or complaint, an auditing procedure, or proactive monitoring. Fraud is even discoverable by chance.

Because tips are one of the most valuable resources for discovering internal fraud, companies should encourage them by implementing easily accessible and anonymous (where permitted by law) fraud reporting tools, such as a tip hotline or dedicated web page. Additionally, these reporting programs should be designed to accept tips from external sources, such as customers and vendors.

Not all tips are valid, and while it is important to consider the motives of individuals willing to supply information of this kind, all tips must be approached as if they will provide useful information. In many instances, the tipster provides information that is of value in commencing an internal fraud examination.

The appropriate response varies depending on the facts, such as the underlying evidence, who is implicated, and the origin of the evidence (e.g., internal sources, civil lawsuit, investigation by the government).

When evidence of fraud arises, management generally should respond by engaging in the following actions:

- Activating the response team
- Engaging legal counsel, if necessary
- Contacting the insurance providers if it makes sense to do so
- Addressing immediate concerns (e.g., preserving relevant documents and identifying who should be informed about the allegation)
- Conducting an initial assessment to determine the appropriate response
- Documenting the initial response

Activating the Response Team

When evidence of fraud arises, management must activate the fraud response team—the group of people tasked with responding to incidents of fraud. The response team should seek to answer the following questions:

- Is a formal investigation necessary?
- If a formal investigation is necessary, who will lead it?
- Is there a need for immediate police involvement?
- Is there an immediate need for legal assistance or advice?
- Is there a need for external support (e.g., forensic specialists)?
- Is there a need for additional support (e.g., access to IT facilities or a secure room, support from administration)?
- Is there a need to devise a media strategy to deal with the issue?
- Is there a need to report the issue to an external third party?
- Should the audit committee be informed?

Engaging Legal Counsel

Because of the legal uncertainties associated with certain instances of fraud, management should consult with internal and possibly external local legal counsel before making any decisions or taking any action concerning the suspected conduct. Typically, an organization's general counsel should be made aware of any significant fraud that might result in legal action.

Fraud examiners should also consult with legal counsel regarding the specific laws and regulations applicable in the relevant jurisdiction that might affect their investigation, particularly the way they conduct interviews. Interviews—especially those of suspected parties—might expose the company and the fraud examiner to certain legal risks.

For specific information on legal considerations when conducting a fraud examination, refer to the "Legal Issues in Conducting Investigations" chapter in this section of the *Fraud Examiners Manual*.

Contacting the Insurance Providers

When evidence of fraud arises, it is difficult to know whether the incident will result in an insurance claim, but, even so, many insurance policies require timely notice of potential claims. Therefore, an organization should consider putting its insurer on notice to preserve a potential insurance claim.

Addressing Immediate Concerns

When evidence of fraud arises, management and the response team should address immediate concerns, which might include:

- Preserving relevant documents
- Identifying who should be informed

Preserving Relevant Documents

When evidence of fraud arises, management should seek to preserve all relevant documents, especially those that an employee might want to hide or destroy. In a fraud investigation context, the term *documents* typically refers to but is not limited to: contracts, invoices, correspondence, memoranda, weekly reports, presentations, telephone messages, emails, reports, performance reviews, performance improvement plans, medical records, and other written or recorded material.

When evidence is misplaced, lost, or destroyed, it becomes more difficult to investigate. Thus, the response team and management must take action to preserve evidence as soon as the decision to investigate is made. There are a number of steps that management should take to preserve relevant documents. First, management should work with legal counsel to issue a litigation hold to notify employees to suspend the destruction of potentially relevant records. Furthermore, management should temporarily suspend the organization's record retention policy to avoid evidence accidentally being destroyed.

Also, management could restrict access to emails or digital files that employees might want to conceal or destroy. Digital information can be found in virtually any type of media, and it is more fragile than tangible evidence. Therefore, employees can destroy this type of information if it is not protected properly. Often, when fraudsters become aware of an investigation, they try to destroy evidence in their computers or sabotage other evidence that could be used against them. Accordingly, it is generally a good idea to have IT personnel involved in this process each time the organization decides to investigate.

The failure to preserve documents could have several adverse consequences. First, it could cast doubt on the integrity of any fraud investigation. Second, documents destroyed when litigation is expected or in progress might result in obstruction charges or allegations of spoliation, which, if proven, could lead to the imposition of sanctions. *Spoliation* is broadly defined as "the intentional or negligent destruction or alteration of documents relevant to litigation."

In today's digital environment, digital spoliation is a major concern for organizations involved in legal proceedings. When compared to the spoliation of tangible documents, digital spoliation carries additional risks. Management often lacks sufficient knowledge of the inventory of digital information, and electronic data might only be available for a brief time, as described earlier in this chapter in the "Litigation Hold Procedures" section.

Identifying Who Should Be Informed

Management and the response team should identify whom to inform about the initiation and progression of the investigation. Depending on the facts, several departments should be interested in a potential fraud allegation, including legal, human resources (HR), internal audit, security, risk management, and loss prevention. When responding to an allegation of fraud, it is important to consider the interests of each of these departments to ensure that designated employees are notified immediately and to enable a prompt response. Information about incidents, however, should be shared only on a need-to-know basis.

HR personnel address issues involving unfair treatment, discrimination, harassment, substance abuse, or corporate policies. Therefore, the HR department should be informed of fraud that involves or affects any such areas.

Both the HR and legal departments should be notified to ensure that the right people receive information in a timely manner. Also, other departments—such as loss prevention, risk management, audit, and security—might need to be notified. Although the development of information distribution rules requires the participation of several departments, it is best to have these rules set before investigation protocols are in place.

Another department that typically needs to be informed is the IT department, because they might need to be part of an investigation to safeguard data until the information can be analyzed. IT personnel can also help identify what data is available and where, and they might be able to function as digital forensic experts if licensed to do so. If a member of the IT department is suspected of being involved in a fraud, extra care should be taken to ensure that engaging the department does not tip off the suspect and create opportunity for the deletion or spoliation of digital evidence.

Again, management must restrict access to certain pieces of information on a need-to-know basis.

Conducting an Initial Assessment to Determine the Appropriate Response

Usually, when an allegation of fraud arises, there are not enough known and verified facts to begin a formal investigation; therefore, management and the response team should conduct an initial assessment to determine whether an investigation is needed and what steps are required, if any, to respond in an appropriate manner. This is perhaps the most critical question that management must answer when an allegation of fraud arises.

An initial assessment should be quick and unless complications arise, completed within a few days. Ideally, action should be taken within three days of learning about an incident.

The initial assessment should be a limited fact-finding analysis focused on the specific allegation or incident. Unlike a formal investigation, it does not require an investigation plan or report. Thus, the initial assessment should seek to:

- Determine if fraud occurred.
- Identify the status of the fraud (e.g., When did it begin? Was it internal or external? Is it still occurring? If it is no longer occurring, when did it stop?).
- Identify potential claims and offenses.

To conduct an initial assessment and determine the appropriate response, the personnel specified in the response plan should take the following steps:

- Understand the context.
- Review any applicable policies and procedures.
- Investigate the allegations.

Understand the Context

Those responsible should gain an understanding of all the circumstances leading up to the current situation. Often, the context is necessary to determine the best approach to dealing with a tip or suspicion, and it can provide clues that are helpful in other areas. Efforts to understand the context should seek to obtain the initial facts and circumstances about:

- The manner in which the suspicions became known
- The date suspicions became known
- The areas to which the suspicions pertain
- The source of the information
- The allegations at issue

Review Any Applicable Policies and Procedures

Those involved in the initial assessment must also review any applicable internal controls and organizational policies, including any anti-fraud auditing and testing policies and procedures, to determine the best method and processes for continuing the investigation.

Investigate the Allegations

An initial assessment should be a limited, fact-finding analysis, and it should focus on investigating the specific allegation or incident. More specifically, to determine the appropriate response, the assessment should, if possible, seek to answer a number of questions regarding the allegation, including:

- Is the allegation credible?
- Who is the subject of the allegation, and what is their relationship to the company?
- When did the alleged misconduct occur, and how often did it occur?
- What was the business purpose of the activity related to the allegation?
- How serious is the allegation?
- What levels of employees are alleged to be involved in the misconduct (i.e., officers, directors, or managers)?
- What individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?
- Did any third parties receive any direct or indirect benefit from the alleged misconduct, and if so, who are they?
- If a third party is involved, is the third party a government official?
- How was the matter recorded on the company's books and records, if applicable?
- Can it be determined whether the person in question acted with fraudulent intent?
- Is it possible that the issue might be larger than reported?
- Were there any whistleblowers, and if so, how should they be handled?
- What measures should the company take to document how the initial evidence of wrongdoing was handled?
- Is the government already involved, and if not, is it likely that the government will become involved?
- Is it likely that the matter will have a significant negative impact on shareholder value?

These questions are important because the response should be proportional to the potential scale of the fraud in terms of its value, frequency, potential damage, the individuals involved, and the number of people involved.

In addition, the decision as to the appropriate response will be influenced by other factors. As with any business decision, the cost of investigating must be considered, and management might also consider whether and to what extent an investigation will interrupt business activity.

Generally, the investigation portion of the initial assessment involves:

- Contacting the source if the investigation was triggered by a report or complaint
- Reviewing key evidence
- Interviewing key individuals

CONTACTING THE SOURCE

If the initial evidence came in through a tip from an identified source, those responsible should contact the source to find out additional information and confirm the source's willingness to help throughout the investigation.

When contacting the source, the interviewer should encourage the complainant to provide a narrative description of the report. After the source provides the narrative, the interviewer should ask clarifying questions and then summarize the key points.

An interview with the source should seek to answer the following questions:

- What does the individual know?
- How did the individual get the information?
- Who were the key individuals involved?
- When did the alleged events occur (e.g., dates, times, and locations)?
- What are the details (e.g., who, what, when, where, why, and how much) of the allegations?
- What are the dates (or period) of the key events?
- What evidence exists to corroborate the alleged events, where is the evidence located, and how can the evidence be accessed?
- What witnesses can corroborate the alleged events?
- Which individuals might have pertinent information about the matter that would tend to support or refute the complainant's position, and what facts do these individuals purportedly know?
- What was the motivation behind the alleged events?
- Why were the alleged actions improper?

- If the scheme is ongoing, do the subjects know of the complainant's report?
- What is the complainant's motivation for making the report (e.g., what prompted them to report this)?

When interviewing the source, the interviewer should seek to determine whether there is any reason to suspect the complainant's credibility. Also, if there are any critical components missing from the complainant's information, the interviewer should ask the complainant to explain what they expect the subject would say in defense of the allegations and ask the complainant to explain why such a response is not sufficient to dispose of the matter. Additionally, the interviewer should ask the source what they want or expect the organization to do about the complaint. The response to such an inquiry will help the team focus its efforts.

REVIEWING THE EVIDENCE

Another crucial part of the initial assessment includes the review of relevant documents and files, which might include personnel files, the organization's employee handbook, accounting records, vendor activity reports, budget reports, fixed asset records, expense reimbursement records, leasing documents, rental agreements, payroll records, purchasing requisitions, purchase contracts, inventory records, shipping and receiving reports, emails, telephone records, and documents from external sources. Some of these documents may have already been reviewed as part of understanding the context of the investigation.

Obtaining and reviewing these documents will assist in understanding the chronology of events and might put the responsible parties on notice as to certain strengths or weaknesses of the investigation. It will also develop information that should be used when interviewing key individuals.

INTERVIEWING KEY INDIVIDUALS

Those responsible for the investigative portion of the initial assessment should interview key individuals for information about the suspicious conduct and the subject(s). Interviewing individuals with personal knowledge is critical.

Also, they should interview witnesses as early as possible because it limits the harm arising from loss of memory, witnesses becoming unavailable, and inadvertent loss or destruction of key evidence.

Documenting the Initial Response

To avoid any real or perceived minimization of the matter's significance and any attempts at willful ignorance (i.e., consciously avoiding important facts to avoid criminal liability), the actions and findings of the initial assessment should be documented. In addition, management must document its initial response and the reasons behind it. Thus, if management decides against investigating, it must document the reasons why.

Again, as soon as a suspicion of fraud arises, management should document the organization's initial response in an incident report log that serves as a record of the organization's response efforts. As the issue progresses, the log should be modified and ultimately should contain details of actions taken and conclusions reached.

The incident report log should contain all information relevant to or created during the initial response that is used to support management's decision-making.

Planning and Conducting a Formal Investigation

Once it is determined that an allegation or issue will be investigated, those responsible must begin the formal investigation. Typically, the steps involved in this process include:

- Completing engagement letters or contracts
- Issuing advisory letters
- Assembling an investigation team
- Learning about the organization at issue
- Developing an investigation plan

Completing Engagement Letters or Contracts

CFEs are sometimes hired for specific engagements, and in such cases, it might be preferable to document the engagement in a formal written contract or a client engagement letter. (In some circumstances, an oral understanding might be sufficient.)

Engagement letters or retainer agreements are beneficial for various reasons. First, they maximize a fraud examiner's protection in the event of a client dispute or misunderstanding, making later disputes about the engagement's terms easier to resolve. Additionally, they help manage client expectations by making the assignment's objectives and the fraud examiner's authorizations and responsibilities clear. It is important to note, however, that although formal, written agreements might be preferable, they are not always practical.

Engagement letters should be written with certain standards in mind, and they should address a variety of items. Those items include but are not limited to: the client's identity, the scope of the services, the timing of the work, deliverables, payment terms and fee structure, communication with the client, non-guarantee, governing law, jurisdiction, termination, and a limitation of liability through indemnity clause.

Examples of engagement letters can be found in Appendix A (located in this section of the *Fraud Examiners Manual*).

Engagement letters generally contain the following basic parts:

- Opening
- Body
- Terms
- Indemnity clause
- Close

Opening

The opening paragraph should state the purpose of the engagement. It should be specific as to whether the letter is an engagement or a proposal letter.

Body

In the body of the engagement letter, the fraud examiner typically describes the procedures and scope of an examination to the extent appropriate for the individual engagement. The amount of detail regarding the described procedures depends on the type of engagement. Engagements that require the investigation of fraud allegations and a concluding opinion on the existence of fraud will typically feature a shorter body that focuses more on the allegations prompting the engagement rather than specific procedures the fraud examiner expects to perform.

At the onset, the fraud examiner might not know what procedures will be necessary to resolve the allegation, and in such circumstances, it is difficult to describe the anticipated procedures with any precision. Therefore, the body of the engagement letter might state that the services will include an investigation of a fraud allegation received over the hotline, by an anonymous tip, or by an audit anomaly. It might also confirm whether the fraud examiner has access to any personnel or documentation deemed necessary to execute the assignment.

An engagement letter for a review of an organization's anti-fraud policies and controls might feature a longer body that specifically describes procedures to be performed and limits the scope of the examination to the procedures mentioned.

Terms

The terms paragraph of an engagement letter should include the payment terms; fee structure; method of payment; a retainer, if needed; and how many hours of examination time the client initially agreed upon.

Additionally, this section should describe the billing procedures and a statement regarding payment methods.

Also, the terms should address out-of-pocket expenses. If travel is required, for example, the terms should discuss the anticipated cost of travel and the number of trips.

This section should include:

- The fraud examiner(s) assigned to the case.
- The fraud examiner's hourly rate (if billing at a flat rate).
- If there is a retainer, the terms section should include a statement regarding the exhaustion of the retainer, what expenses will be reimbursed if there are unused retainer proceeds, and when and how such reimbursements will be refunded.
- A policy regarding past due invoices and late fees, including finance charges if applicable.
- Rates for any additional services or expenses that might be needed.

Indemnity Clause

In letters of engagement, there should be an indemnity clause to protect the fraud examiner if the subject, a witness, or a third party sues the client and includes the fraud examiner as a party to the suit. The clause should be tailored to fit the particular terms of the engagement.

The indemnity must be broad enough to cover the fraud examiner's legal expenses, provide for independent counsel, and protect the fraud examiner from liability in case of an adverse finding, but it should also provide for the cost of time and expenses of the fraud examiner at the fraud examiner's usual hourly rate.

SAMPLE INDEMNITY CLAUSE

[Client company] agrees to indemnify and hold harmless [fraud examiner's company]—including its personnel, agents, subcontractors, and consultants—from and against any and all claims, liabilities, cost, and expenses, including labor arbitration or related proceedings (including without limitation, independent legal representation of [fraud examiner's company]'s choice and attorney's fees, plus the time of [fraud examiner's company] personnel, operatives, and consultants involved to defend or appear at any judicial or quasi-judicial proceedings) brought against, paid by, or incurred by [fraud examiner's company] as a result of any of its services provided to [client company] in this project.

This includes, but is not limited to, any claims arising from violations of any laws relating to personal injury or property damage whatsoever suffered by [client company], its employees, or third parties. This provision shall survive the termination of this agreement.

Close

The closing section should conclude the letter. It should thank the addressee for the opportunity, and it should include the fraud examiner's contact information.

Also, the closing should include the date of agreement, client's signature, printed name, client's contact information, and the fraud examiner's signature. The fraud examiner should ask the addressee to sign one copy and return it.

Issuing Advisory Letters

An individual or organization can use an advisory letter to convey information intended to inform or state an opinion about an issue relevant to a client or member base. These letters include an auditor's formal opinion concerning a company's financial operations, an attorney's opinion regarding a particular point of law, or a fraud examiner's general findings as to the presence of fraud or lack thereof. Several examples of fraud examination advisory letters can be found in Appendix A.

Assembling an Investigation Team

Fraud examinations usually require a cooperative effort among different areas of expertise; therefore, if members of management decide to investigate suspicions of fraud, they must determine who should lead and be involved in the investigation.

To determine this, management must identify the needed skills. Typically, fraud investigations require skills across different areas of expertise and industry sectors. Auditors, fraud examiners, managers, attorneys, IT personnel, and security personnel are frequently associated with fraud investigations.

Selecting the right team members is essential for an effective fraud examination. Accordingly, when choosing the participants for an investigation team, it is critical to identify those who can legitimately assist in the investigation and who have a legitimate interest in its outcome. Only these persons should be included on the investigation team.

Also, when organizing the team, it is important to consider all of the implications that might arise from an investigation. These implications include the business, legal, human resources (HR), and operational factors that arise when an investigation commences. Addressing these potential issues before the investigation begins ensures that significant factors (e.g., the team members' abilities, the leading executives, and the assurance of independent action and reporting) are considered.

Furthermore, the team should comprise professionals with the skills needed to help solve various types of incidents. To acquire the appropriate level and combination of skills, the team should include internal resources (if available) and external resources (if needed or appropriate).

Typically, team members should have:

- Accounting and audit knowledge
- Knowledge of the industry
- Knowledge of the organization
- Knowledge of the law and the rules of evidence in the jurisdiction(s) where the fraud allegedly occurred
- Knowledge of privacy issues in the jurisdiction(s) where the fraud allegedly occurred and where the investigation will occur
- An understanding of psychology and motivational factors
- Interviewing skills that are in the relevant language(s)
- Communication skills
- Knowledge of, and experience with, relevant technologies

A successful fraud examination, however, depends not only on the knowledge and skills of individual members but also on the individual team members' characteristics that facilitate team interaction and functioning. These characteristics are especially critical for teams that require more coordination.

After identifying the necessary skills and characteristics, management must determine who possesses them and begin selecting the team. Each team varies, depending on the goals, circumstances, and people involved.

Common Types of Professionals

A typical fraud examination team might include the following types of professionals:

- CFEs
- Legal counsel
- Local international counsel
- Accountants or auditors (internal or external)
- Forensic accountants
- Audit committee members
- Security personnel
- HR personnel
- A management representative
- IT personnel
- Digital forensic experts
- Data analytics specialists
- External consultants
- Industry specialists

CERTIFIED FRAUD EXAMINERS

CFEs are trained to conduct complex fraud cases from beginning to end. A CFE has training in all aspects of a fraud examination and can therefore be valuable in bringing together the financial examination and the more traditional investigative techniques.

LEGAL COUNSEL

It is crucial to have legal counsel involved in and, in most cases, leading fraud examinations, at least regarding the legal aspects of the process. This is because a fraud examination can generate many legal questions, and the team must have legal counsel available to help answer these questions. Otherwise, the investigating organization risks exposing itself to greater

danger than the threat it is investigating. Legal counsel can have an important role in reporting results, preserving confidentiality, avoiding lawsuits, or terminating employees for wrongful misconduct.

In addition, by having an attorney lead or oversee the investigation, the company might be able to protect the investigation's confidentiality under certain evidentiary privileges (e.g., the attorney-client privilege in the United States and the legal advice privilege in the United Kingdom) and similar forms of protection that shield certain types of evidence from being discovered or produced during trial.

LOCAL INTERNATIONAL COUNSEL

Management should obtain the help of local international counsel before beginning a fraud investigation involving work abroad.

Local international counsel is needed to help resolve a number of issues that occur when working in foreign jurisdictions. For example, local counsel can provide advice concerning applicable privileges and guidance as to whether local laws afford employees privacy rights that might interfere with the investigation.

ACCOUNTANTS OR AUDITORS (INTERNAL OR EXTERNAL)

As knowledge of accounting and auditing is necessary for most fraud examinations, a team might include accountants or auditors, whether internal or external. Auditors can support the investigation with information on company procedures and controls. Internal auditors are often used to review internal documentary evidence, evaluate tips or complaints, estimate losses, and assist in technical areas of the company's operations. Additionally, auditors can assess the probable level of complicity within the organization, and they can help design procedures to identify the perpetrators and help determine the extent of the fraud.

FORENSIC ACCOUNTANTS

A forensic accountant can provide various services, including audits; accountant performance reviews; and examinations of financial documents for fraud, misconduct, or industry standard violations. Moreover, these experts can mine and analyze large amounts of data to identify potentially irregular transactions and high-risk relationships.

AUDIT COMMITTEE MEMBERS

In recent years, audit committees have taken a more active role in internal investigations. This has occurred, in part, because legislation such as the Sarbanes-Oxley Act (SOX) in the United States and similar legislation in many other countries mandates that audit committees for publicly traded companies be directly responsible for two key components of an effective fraud prevention program—outside audits and internal reporting mechanisms. Accordingly, a company's audit committee might actively oversee a fraud examination or require that the investigation team report directly to it.

SECURITY PERSONNEL

Security department investigators are often assigned the investigation's fieldwork responsibilities, including interviewing outside witnesses and obtaining public records and other documents from third parties.

HUMAN RESOURCES PERSONNEL

The HR department should be consulted to ensure that the laws or internal policies governing the rights of employees in the workplace are not violated. Such involvement will lessen the possibility of a wrongful discharge suit or other civil action by employees. Also, involving HR personnel can help provide access to the organization's policies and any employee information that might be needed. Moreover, HR can help the team understand office procedures and place suspect employees on paid leave if necessary.

Although the team might need advice or assistance from an HR specialist, normally this person would not directly participate in the investigation.

MANAGEMENT REPRESENTATIVE

A representative of management or, in significant cases, the audit committee of the board of directors should be kept informed of the progress of the investigation and should be available to lend necessary assistance.

INFORMATION TECHNOLOGY PERSONNEL

If fraud occurs, it is likely that a computer or other electronic device was involved. If so, IT personnel might need to be part of an investigation to help identify what data is available and where it is located, as well as to help safeguard the data until it can be analyzed.

DIGITAL FORENSIC EXPERTS

When developing a fraud examination plan, management should determine whether a digital forensic expert is needed.

In today's world of evolving technologies, more and more information is created, stored, and disseminated electronically. Due to the sensitivity of digital evidence, a fraud examination team should include a digital forensic expert if an investigation involves more than a brief analysis of electronic evidence. Moreover, with the majority of communication being conducted electronically, emails and other digital communications can and will be used as evidence in almost any case.

Digital forensic experts can uncover a large amount of data that relates to the use of a computer or other electronic device, what is or has been stored on it, and the details about the device's users. Additionally, digital forensic experts might be able to recover evidence that a nonexpert cannot. For example, if the target of an investigation tries to delete electronic evidence, a digital forensic expert might be able to recover the deleted files, depending on when and how the files were deleted. Similarly, a digital forensic expert might be able to bypass encrypted information.

Also, it is important to allow a trained examiner to conduct a proper seizure and examination of digital evidence to help ensure that the information can be used in a legal proceeding if necessary. Within the digital forensics field, there are several different types of experts. Given the diversity of computer-related fraud, no person can be an expert in all aspects of computer technology.

In cases involving litigation, a digital forensic expert can help parties draft interrogatories and requests for the production of evidence designed to solicit relevant data, as well as help prepare and participate in depositions involving record custodians.

DATA ANALYTICS SPECIALISTS

As the volume of electronic records continues to grow, it is increasingly necessary for investigation teams to include data analytics specialists. These specialists are adept at searching, collecting, extracting, cleansing, analyzing, and modeling data. Thus, data analytics specialists can help manage costs, especially in larger, more complex investigations.

EXTERNAL CONSULTANTS

When conducting a fraud examination, fraud examiners should determine whether a technical specialist or other subject-matter expert is needed.

When the suspect employee is particularly powerful or popular, it might be useful to involve outside specialists who are relatively immune from company politics or threats of reprisals.

INDUSTRY SPECIALISTS

In some cases, it might be necessary to include an individual with extensive industry knowledge. Industry specialists can help develop the investigation plan, evaluate technical documents, and identify potential misstatements by interviewees.

Dos and Don'ts for Selecting Team Members

When selecting team members, it is best practice to:

- Consider the team's size.
- Check for conflicts of interest between internal and external team members and parties relevant to the investigation.
- Ensure that there are no reporting issues (e.g., a team member feels pressure to report all details of the investigation to their direct manager, even though their manager does not have a need to know). Reporting issues can be prevented by establishing confidentiality rules at the beginning of the investigation.
- Select team members who fit the investigation's demands and objectives.
- Recruit team members with the skills needed to conduct the investigation.
- Recognize the unique knowledge, experience, and skills that each team member can contribute.
- Contemplate the ways that each potential member will fit into the team.
- Select people who will work well with other team members.

The following behaviors should be avoided when selecting team members:

- Select team members based on friendship.
- Select team members to repay a favor.
- Select team members with negative attitudes.
- Overlook team members with untraditional knowledge that can contribute to the investigation (e.g., people with experience in a particular industry).
- Select team members who might have personality conflicts with other members.
- Select team members with a vested personal or corporate interest in the matter.

- Select team members with a close personal or professional relationship with the subject or the complainant.
- Select team members who lack restraint and a sense of discretion.

Identifying the Investigation Leader

When evidence of fraud arises, management must designate someone to lead the investigation. A leader should have investigative experience and knowledge of legal and compliance requirements regarding the specific issues involved.

The investigation leader should be determined based upon the seriousness of the allegation. Management should consider whether to appoint an internal party (if available) or an external third party to lead and oversee the investigation.

The leader should be independent of the activity affected by the alleged fraud and have the means to recruit resources necessary to conduct the investigation, sufficient authority and access to gather any necessary information, and the ability to communicate with senior management.

Learning About the Organization at Issue

When tasked with conducting a fraud examination involving an organization, the team must become familiar (if it is not already) with the organization, as well as its industry, competition, market share, financing structure, vendors (suppliers), customers, receipt (i.e., cash or on account) and disbursement methods, procurement methods, economic climate, recordkeeping system, policies and procedures, employee organization chart, job responsibilities of key employees, and other matters that might be relevant to the fraud examination.

Understanding the entity will enable the team to assess the risks associated with the entity's particular operations.

Developing an Investigation Plan

Once it is determined that an allegation or issue will be investigated and the investigation team has been assembled, the team should develop an investigation plan.

Each member of the team should be involved in the planning process. Letting each team member contribute to the planning process increases the likelihood that everyone will accept the plan and results in a team approach that draws on each member's expertise.

The team should start planning early and update the plan throughout the investigation. Planning is not a one-time event: it is an ongoing process that requires constant attention. The team must refine its plan as the facts and needs change.

Each fraud investigation is different, and no single plan can cover every situation. The facts and circumstances of each case should shape how an investigation is structured, what procedures are performed, and how those procedures are executed. Nevertheless, it helps to have a standard set of items from which to begin the planning process.

In short, when developing an investigation plan, those responsible should:

- Review what is known and gain a basic understanding of key issues.
- Define the goals of the investigation.
- Identify whom to keep informed.
- Determine the scope of the investigation.
- Establish the investigation's time frame.
- Assess the need for law enforcement assistance or notification.
- Define members' roles and assign tasks.
- Address operational issues.
- Outline the course of action.
- Adapt the necessary resources to conduct an investigation.
- Prepare the organization for the investigation.

Review What Is Known and Gain a Basic Understanding of Key Issues

The known information should serve as the basis for the investigation plan. Before writing the plan, the fraud examiner must review what is known and gain a basic understanding of issues that are key to planning the investigation.

Typical questions to answer before beginning a fraud examination include:

- What period is under review?
- What is the time frame?
- What are the deadlines?
- What is the nature of the suspected fraud?

- Where are the relevant locations?
- Who is the contact at the locations?
- Who are the person(s) of interest?
- Does the issue predate any of the key players?
- Have any related fraud examinations ever been conducted at the relevant location?
- What other entities, departments, or regions might be involved?
- How long has the issue existed?
- What is the culture of the industry or department at issue?
- What other sites might be involved?
- Does the organization perform background checks on employees as a precondition of employment?
- Did the suspected fraud occur in an industry or location that has a history or culture of fraud?
- Has the organization been in compliance with reporting and regulatory requirements?
- What is the profitability of the unit or organization at issue in the investigation?
- Does the organization's level of growth make sense in light of its industry and peers?
- Has there been a recent acquisition and, if so, is former management still in place?
- Does the organization have a fraud policy?
- What type of report (written or oral) does the client expect?
- What is the budget?

After obtaining a basic understanding of the key issues, the fraud examiner can begin developing the investigation plan.

Define the Goals of the Investigation

An investigation must have goals, which should be identified at the outset so the team members can design the investigation to achieve them. Goals also help keep the investigation focused, and they can serve as a motivator as long as they are specific, well-defined, and measurable. A specific goal is more likely to be achieved than a general goal, and goals must be realistic within the availability of resources, knowledge, and time. Measurable goals will allow the team to determine attainability, estimate a timeline, and know when the goals have been achieved.

Although the basic goal for most fraud investigations is to determine whether fraud occurred—and if so, who perpetrated it—fraud investigations might be designed to achieve a number of different goals, such as to:

- Prevent further loss or exposure to risk.
- Determine whether there is any ongoing conduct of concern.
- Establish and secure evidence necessary for criminal or disciplinary action.
- Minimize and recover losses.
- Review the reasons for the incident, assess the measures taken to prevent a recurrence, and determine any action needed to strengthen future responses to fraud.
- Help promote an anti-fraud culture by making it clear to employees and others that management pursues all cases vigorously and takes appropriate legal or disciplinary action where it is justified.
- Protect the company's legal privileges.

Identify Whom to Keep Informed

The investigation team and management must identify who should be kept informed about the investigation at the outset of a fraud examination. In general, it should be as few people as necessary.

Factors to consider when determining who should be kept informed include the severity of the incident being investigated, the main suspect's role in the organization, and the tasks that will be required to conduct the investigation.

Determine the Scope of the Investigation

When planning an investigation, the stakeholders should identify the *scope* (the boundaries or extent of the investigation), which will vary depending on the facts and circumstances. An investigation, for example, might be limited to the subject matter, the department, or the geographic area at issue.

To determine the scope, those responsible should use the following guidelines:

- Consider the ultimate goals of the investigation.
- Develop a list of key issues raised in the initial assessment.
- Determine the level of discretion that is required.
- Determine whether there are any constraints (e.g., time, resource, authority, procedural, legal, or practical). Identifying such limitations helps ensure that the team can meet realistic objectives and develop alternative strategies.
- Consider the quality of the organization's anti-fraud program and policies.
- Consider the organization's actual culture of compliance.

- Determine the extent to which mid- and senior-level management is involved in the suspected misconduct.
- Determine whether the issue is widespread or isolated to a particular area.
- Ascertain whether the suspected misconduct was prohibited by the organization's compliance program.
- Consider broadening the scope if the allegations indicate a failure in the organization's compliance program.
- Consider what the government expects or requires.
- Evaluate the feasibility of in-person versus remote investigation processes.

Additionally, to determine the scope, the team and management should consider how the issue became known (i.e., what prompted the investigation). Fraud issues can stem from a number of sources, and different sources prompt different responses. If, for example, the issue arose from a government investigation, the company's investigation should closely examine the government's actions.

Establish the Investigation's Time Frame

When planning the investigation, the team must establish proper time parameters with start dates and due dates for tasks and deliverables. Also, the team should obtain the dates of upcoming earnings releases and audit committee meetings.

An established time frame helps the team provide a quick and appropriate response, which enables the subject organization to avoid future legal disputes and minimize adverse impact on employee morale. Some circumstances might not allow for a quick response, such as situations requiring extensive investigations of multiple allegations; therefore, the time required to accomplish necessary tasks must be thoroughly considered when setting the parameters.

Time parameters, when realistic and appropriate, help the team members structure their plans, providing information to help develop concrete, short-range actions to reach the investigation's goals.

Assess the Need for Law Enforcement Assistance or Notification

The planning stage of the investigation should also include efforts to consider the need for law enforcement assistance or notification. That is, management must decide whether the matter at issue is serious enough to call in the police or other law enforcement entities.

Whether to seek assistance from law enforcement can be a difficult decision for organizations to make. Some situations require that law enforcement be notified, depending on the nature of misconduct and the jurisdiction in which it occurs.

If, at the beginning of the investigation, management determines that it will make a formal referral to law enforcement or a prosecuting agency, then it must notify the authorities before the investigation commences to determine whether law enforcement personnel should participate in the examination.

Define Members' Roles and Assign Tasks

If the organization at the center of the investigation does not have a pre-established line of authority in its fraud policy or investigative protocols, the team members' authority levels, responsibilities for action, and reporting lines should be defined during the investigation planning process. For efficient and effective coordination, all team members must be clear about their roles and responsibilities and how they relate to the investigation's goals. Also, defining the members' roles and responsibilities gives them purpose and checkpoints for measuring success.

Conversely, failure to define roles and responsibilities can have an adverse impact on an investigation. Without clear roles, the team might waste time and money, gaps in the investigation process might appear, or the investigation might lead to incomplete or faulty results.

That said, delineating the team members' roles is difficult because fraud investigations often are conducted in an unstable and high-pressure atmosphere that disrupts communication. Nevertheless, it needs to be a priority for management and individuals on the team.

In general, team members should understand:

- Their expected roles and responsibilities
- The expected roles and responsibilities of other team members
- The degree and source of any outside scrutiny
- Timing issues
- Expected form and timing of interim deliverables or final product
- Specific facts of the matter at issue
- Limitations on who can be involved in the investigation or informed of its specifics

Management should designate a primary contact person with whom the team can communicate on all matters that arise during the investigation. The team must report to someone who will take action pursuant to the investigation's findings.

Address Operational Issues

During the planning process, management must consider any operational issues, which might include:

- Gathering facts abroad
- Recordkeeping practices abroad
- Record content and format differences
- Remote work considerations
- Language translation
- Cultural differences
- International data privacy issues
- Differing conceptions of privacy and discovery
- Immigration regulations
- Safety concerns, especially for global assignments

Among the issues listed, international data privacy laws are of particular concern. Many foreign countries—and those in the European Union (EU) in particular—restrict or prohibit processing and transferring personal data. For example, the EU's General Data Protection Regulation (GDPR) requires notice and consent before collecting or processing personal data and in most cases, limits the transmission of personal data to non-EU countries. For more information on the GDPR, see the "Legal Issues in Conducting Investigations" chapter in this section of the *Fraud Examiners Manual*.

Similarly, because recordkeeping practices in other countries differ, difficulties can arise when attempting to obtain information in foreign countries.

Additionally, with more organizations embracing remote work for their employees and decreasing travel budgets, the multi-jurisdictional nature of many organizations' operations has caused fraud examiners to be tasked with conducting their engagements remotely.

Determining which functions can be performed remotely and adapting the investigative plan accordingly is increasingly common. Fraud examiners might need to engage local

professionals to execute tasks that cannot be performed remotely, such as conducting interviews or gathering physical copies of documents.

For more information on conducting interviews remotely, see the content on "Remote Interviews" in the "Interview Theory and Application" chapter in this section of the *Fraud Examiners Manual*.

Outline the Course of Action (Case Plan)

Before the evidence-collection phase of a fraud examination begins, the investigation team should develop a case plan to make sure it addresses every relevant issue identified thus far. A case plan outlines the course of action the team members expect to take throughout the investigation, and establishing a case plan helps the team stay on track and focus on the key issues.

The case plan can encompass matters such as:

- The scope of the investigation
- The goals of the investigation
- Time parameters
- Resources needed
- Task assignments
- The overall approach to conducting the investigation

Also, the case plan should outline how and in what order the team will proceed. Team members should organize an investigation by breaking it down into smaller, more manageable components. It is important, however, to avoid excessively breaking down an investigation because doing so can lead to micromanagement or inefficient work management.

Investigations are often organized in the following ways:

- *Chronologically*—A chronological investigation is divided into time-based phases that, when completed, are marked as milestones. The phases are the broad steps needed to complete the investigation, and each phase contains tasks that define the actions needed to reach each milestone. The tasks within each phase should be assigned based on who is best suited to perform them. Milestones indicate the investigation's overall progress. This structure is best suited for investigations where time sequence is essential in organizing tasks.

- *By functional area*—This approach organizes investigations by functional areas needed to accomplish the investigation's goals. Thus, this approach focuses on the type of activities and processes that must be done under each functional area.
- *By team member*—This method involves organizing the investigation's work by each team member's area of expertise.
- *Hierarchically*—This approach organizes the team members' roles and tasks hierarchically, from major undertakings to minor undertakings. Thus, the components are organized based on their relationship to each other and assigned based on pre-established lines of authority or reporting.

Because the case plan should outline how and in what order the team will proceed, it should identify the information that is necessary to complete the investigation and include the investigative activities to be performed, such as:

- Documents and evidence that should be located, obtained, and examined
- A list of witnesses and subjects to interview and the preferred order of the interviews
- The date that a report of the investigation should be presented
- Matters that need supervisory review and approval

When developing the case plan, the team should consider:

- How to most efficiently achieve the goals of the investigation
- How to accomplish the goals of the investigation on a timely basis, with appropriate confidentiality and fairness to all parties
- How to ensure that the investigation's results are thorough, accurate, and documented appropriately
- How to ensure compliance with the law and the organization's policies and procedures

The case plan must be adaptable, as circumstances often change and new information emerges throughout an investigation. The team and management should continually refine and modify the plan as needed.

Each stage of the investigation should be documented. Documenting the planning process demonstrates thoroughness, advance thought, and preparation, which will help counter any challenges that the investigation was inadequate or inappropriate.

It is helpful to prepare to-do lists or checklists for an investigation. For reference, a sample checklist is located in Appendix B of this section. The sample checklist, however, is not

intended to cover all aspects of every examination but rather to provide the investigation team with planning assistance.

Adapt the Necessary Resources to Conduct an Investigation

As with any special investigation or operation that requires advance preparation, the planning process in a fraud investigation must include efforts to adapt the resources needed to deal with the variety of issues that might occur during the investigation. A successful fraud investigation requires support from management, the right supplies, adequate funding, and any other identified resources.

That is, the investigation team needs to have the tools necessary to complete the investigation. This is especially true if the relevant operations are in developing economies, remote locations, or areas with a higher risk of security-related incidents.

The necessary resources might include:

- Outside specialists
- Case management software
- Digital forensic tools (e.g., EnCase or Forensic Toolkit)
- Access to a commercial database
- Security arrangements

Also, every team member should have the contact information of all others involved in the investigation.

Prepare the Organization for the Investigation

Before commencing a formal investigation (and especially before starting the evidence-collection process), it might be necessary to prepare the subject organization for the investigation. Preparing an organization for an investigation involves the following:

- Preparing the managers of the employees who will be involved in the investigation, especially if they do not know about the issue, and letting them know that the subject and witnesses might be busy at times during the investigation (The amount of information to share with a manager will depend on the circumstances.)
- Notifying key decision-makers when the investigation is about to begin
- Notifying the organization's in-house or outside counsel when the investigation is about to begin

Generally, it is not good practice to alert all of an organization's employees that an investigation will be taking place, nor should the investigation's purpose be explained to all employees. Even when preparing managers of the employees who will be involved in the investigation, those responsible should not do so by explaining the investigation's purpose, why the investigation is happening, when it is happening, or who else is involved.

Structure the Investigation to Preserve Confidentiality

Fraud investigations must be structured to preserve confidentiality. If confidentiality issues are not given attention from the outset, the details of the investigation might become public, compromising the entire investigation. Additionally, if the details do not remain confidential, employees might be reluctant to report future incidents; if the suspicions that prompted the investigation prove unsupported, the reputations of those suspected of misconduct might be irreparably damaged. Moreover, if an investigation stems from a complaint and the complaint becomes known, then it is possible that there could be retaliation against the complainant.

Accordingly, those responsible must structure the investigation to preserve confidentiality. The team members should:

- Avoid alerting the suspected fraudster(s).
- Request participants' confidentiality.
- Guard case information.
- Consider conducting the investigation under any applicable evidentiary privileges or protections.

Avoid Alerting the Suspected Fraudster(s)

When responding to a sign or allegation of fraud, those responsible must work to avoid alerting suspects.

If the suspect is informed of the investigation, inadvertently or otherwise, a number of different adverse events might occur. For instance, the fraudster might attempt to destroy or alter evidence, making it more difficult to conduct the investigation. When investigation details are leaked, concealment and destruction of evidence typically occur at a faster rate.

Additionally, a forewarned suspect might attempt to flee, cut off contact with associates, make the proceeds of the fraud more difficult to find or recover, or try to place the blame on somebody else.

Since unintentionally notifying the fraudster is a key concern in any investigation, the confidentiality of an internal investigation is critical. To maintain confidentiality, determine in advance who should receive information about the investigation and re-evaluate who should receive information as the investigation proceeds.

The following are some basic measures that organizations and fraud examiners can take to avoid notifying suspects that they are being investigated:

- Know who is being investigated and what they can access.
- Limit the extent of any discussions.
- Inform only those who need to know.
- Inform employees of the consequences of a confidentiality breach.
- Work discreetly without disrupting the office's normal course of business so that employees do not know that an investigation is being performed.
- Work fast.
- Investigate during nonbusiness hours.

Moreover, it is important for fraud examiners to be knowledgeable about the subject organization's guidelines or policies. Do the applicable guidelines or policies have a need-to-know clause and an all-access clause? Such clauses allow the team to keep the details of the investigation confidential and provide access to all the company systems so the fraud examiner can gather as much system evidence as possible without notifying any internal parties.

Finally, if the suspect is alerted, management should adjust the investigation and its timeline accordingly. This might mean interviewing the fraudster out of sequence from a normal investigation.

Request Participants' Confidentiality

To preserve the confidentiality of an investigation, management might (if legally permissible) remind participants to refrain from discussing investigation information with anyone or require participants to sign a confidentiality oath vowing not to divulge any information regarding the investigation.

Generally, an employer can ask employees to keep an investigation confidential when there are legitimate business justifications for making such requests. However, it is usually not wise for management to implement a policy prohibiting all employees from discussing employee

investigations because doing so could violate certain employee rights. Some jurisdictions guarantee private sector employees the right to organize and engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection. If an employer in such a jurisdiction has a routine policy or practice of asking employees not to discuss matters that are being investigated, the policy or practice might violate the employees' right to organize and engage in other concerted activities.

To illustrate, consider the law in the United States. The National Labor Relations Act (NLRA) is the primary labor law in the United States, and it affects an employer's ability to ask employees not to discuss matters that are being investigated.

On June 16, 2015, the National Labor Relations Board (NLRB), the entity that enforces the NLRA, expanded its interpretation of what constitutes protected "concerted activity" under Section 7 of the NLRA. Section 7 guarantees most private sector employees the right to organize and "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." In its decision, the NLRB ruled that an employer's routine policy or practice of asking employees not to discuss matters that are being investigated violates the NLRA, even where the employer did not threaten to take disciplinary action if employees breach confidentiality.

According to the NLRB, employee discussions may be restricted if the employer can show that it has "objectively reasonable grounds" for requiring confidentiality. The decision states that employers must proceed on a case-by-case basis, determining whether confidentiality is necessary based on the circumstances of each case.

The NLRB provided the following suggestions for cases that would validate a legitimate business justification:

- Witnesses needed protection.
- Evidence was in danger of being destroyed.
- Testimony was in danger of being fabricated.
- There was a need to prevent a cover-up.

It is likely that the second, third, and fourth suggestions would apply to most fraud investigations, so fraud examiners in the United States could probably request that employees keep their investigations confidential. Still, it appears that before making a request for confidentiality, fraud examiners should document the need for confidentiality.

Based on the NLRB's decision, U.S. employers should no longer have a policy prohibiting all employees from discussing employee investigations.

Guard Case Information

To help preserve confidentiality, the investigation team members should closely guard case information. The following are some recommended procedures:

- Store all confidential documents in locked file cabinets or rooms accessible only to those who have a need to know.
- Protect all electronic information via firewalls, encryption, and passwords.
- Clear desks of any case information before stepping away.
- Lock computers when leaving workstations.
- Mark all case information, whether tangible or electronic, as confidential.
- Avoid talking about the investigation in public or in any place where other employees can hear the communications.
- Avoid using unsecure email or other electronic means (e.g., text messages or instant messages) to transmit confidential case information.

Consider Implementing Any Applicable Evidentiary Privileges or Protections

To prevent third parties, including the subject of the investigation, from having access to the investigative materials, management should consider conducting the investigation under any applicable evidentiary privilege that provides the right to keep certain information from being disclosed without permission.

If an evidentiary privilege applies to information, the general rule is that the court and the party seeking the information will be denied access to it, and the triers of fact must disregard any evidence they do actually hear if it is deemed privileged afterward; however, legal jurisdictions vary on which communications are protected by such privileges.

Typically, the most relevant types of evidentiary privileges for keeping investigations confidential are legal professional privileges. These privileges protect the communications between professional legal advisors (e.g., solicitor, barrister, or attorney) and their clients, and in some situations, fraud investigations can be structured so that they are afforded protection under such privileges. Generally, to receive protection under a legal professional privilege, a legal professional must direct or supervise an investigation.

In most common law countries, the legal professional privilege is known as the attorney-client privilege, and it protects against involuntary disclosure of communications between clients and their attorneys. The general rule is that the attorney-client privilege only applies to confidential communications (oral or written) between a client and their attorney made for the purpose of giving or receiving legal advice, but courts have extended the privilege to include client communications with nonlawyers (e.g., fraud examiners) who are working under the direct supervision, direction, and control of the lawyer. Specifics of the attorney-client privilege or its analogues might differ from jurisdiction to jurisdiction; local legal counsel should always be engaged to determine applicability of privilege in a fraud examination.

The attorney-client privilege, if properly implemented, typically provides some protection from discovery of internal reports by the subject of the investigation, the government, or third parties. The privilege might also assist in protecting the confidentiality of witnesses. It may not, however, protect the underlying evidence or documents that do not meet the criteria outlined above, and it generally cannot be claimed retroactively to cover work done before counsel was involved.

In addition to legal professional privileges, litigation privileges and other similar evidentiary protections, such as the U.S. attorney work-product doctrine, can protect the confidentiality of investigations. These protections shield materials that are prepared in anticipation of litigation.

The U.S. attorney work-product doctrine, for example, protects tangible materials from discovery that are prepared in anticipation of litigation. To apply this doctrine, litigation must actually be planned, and the work for which protection is sought must have been undertaken for the specific purpose of preparing for that litigation. Also, the protection offered by this doctrine extends to not only information and documents prepared by a party or the party's attorneys but also to information and documents by third-party consultants and examiners hired by the attorneys. For instance, communications with the attorney and any work or analysis conducted by an expert with whom the attorney has consulted is protected as work product; however, this protection will be waived if the expert is called to testify as an expert witness at trial.

For more information on evidentiary privileges and protections, refer to the "Basic Principles of Evidence" chapter in this section of the *Fraud Examiners Manual*.