Investigation

Planning and Conducting a Fraud Examination
Fraud Examination

- *Fraud examination* refers to a process of resolving allegations of fraud from inception to disposition. Tasks include:
  - Obtaining evidence
  - Reporting
  - Testifying to findings
  - Assisting in fraud detection and prevention

- *Forensic accounting* is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation.
Fraud Examination Methodology

- Assume Litigation Will Follow
  - Begin with the proposition that the case will end in litigation

- Act on Predication
  - Should not conduct or continue fraud examinations without proper predication

- Move from General to Specific
  - Informational witnesses first, then subject
Fraud Theory Approach

- Analyzing available data
- Creating a hypothesis
- Testing the hypothesis
- Refining and amending the hypothesis
Develop a Fraud Response Plan

- A *fraud response plan* outlines the actions that members of an organization will take when suspicions of fraud have arisen.
- Because every fraud is different, the response plan should not outline how a fraud examination should be conducted.
- Instead, response plans should help organizations manage their responses and create environments to minimize risk and maximize the potential for success.
Initial Response

- Activate the response team.
- Engage legal counsel, if necessary.
- Consider contacting the insurance providers.
- Address immediate concerns.
- Conduct an initial assessment.
- Document the initial response.
Assemble the Fraud Team

- Certified Fraud Examiners (CFEs)
- Legal counsel
- Local international counsel
- Accountants or auditors (internal or external)
- Forensic accounting investigators
- Audit committee members
- Security personnel
- Human resources (HR) personnel
- A management representative
- Information technology (IT) personnel
- Computer forensic experts
- Data analytics specialists
- External consultants
- Industry specialists
Dos and Don’ts

- Consider size.
- Check for conflicts.
- Check for reporting issues.
- Select team members to fit the demands and objectives.
- Recruit members with the skills needed.
- Recognize unique skills.
- Select people who work well together.
- Don’t select members who lack restraint or a sense of discretion.
Developing an Investigation Plan

- Review 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 timeframe.
- Address the need for law enforcement assistance.
- Define members’ roles and assign tasks.
- Address operational issues.
- Outline the course of action.
- Adapt the necessary resources.
- Prepare the organization.
Prepare the Organization

- Whether or not a violation of the law occurred is not the primary focus – finding the facts is.
- Prepare the managers of the employees involved.
- Notify key decision makers.
- Notify the organization’s in-house or outside counsel when investigation is about to begin.
Preserving Confidentiality

• Avoid Alerting the Suspect
  • Important to have information about the person who is being investigated and what he can access.
  • Limit the extent of any discussions.
  • Only inform 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.
  • Work fast.
  • Investigate during off hours.
Preserving Confidentiality

- Request Participant’s Confidentiality
  - Remind participants to refrain from discussion.

- Guard Case Information
  - Store confidential documents in locked file cabinets or rooms.
  - Avoid talking in public places.
  - Avoid using email or other electronic means (e.g., text messages or instant messages) to transmit confidential case information.

- Consider Implementing Any Applicable Evidentiary Privileges
  - E.g., legal professionals
Sample Prep Question

1. Carter, a Certified Fraud Examiner for Universal Design, learns that Wallace, a shrewd salesperson with an unscrupulous attitude, has close relationships with several Universal Design customers. Carter also knows that Wallace has excessive gambling habits, due in part to his strong desire for personal gain. Carter has sufficient predication to:
Sample Prep Question

A. Directly accuse Wallace of having committed fraud.
B. Alert management that Wallace might have committed fraud.
C. Look for evidence of misconduct in Wallace’s computer and desk area.
D. Conduct discreet inquiries into Wallace’s work as a salesperson.
Correct Answer: D

- 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. *Predication* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, or will occur. If a fraud examiner cannot articulate a factual basis or good reason for an investigative step, he should not do it. Therefore, a fraud examiner should reevaluate the predication as the fraud examination proceeds.
Sample Prep Question

2. Which of the following is the most accurate statement about a fraud investigation plan?

A. An investigation plan should inform employees at all levels about the investigation.
B. An investigation plan should establish the investigation’s timeframe.
C. An investigation plan should establish which individuals violated the law.
D. An investigation plan should make a commitment to eradicate the fraudulent activity.
Correct Answer: B

Once it is determined that an allegation or issue will be investigated, those responsible should develop an investigation plan. An investigation plan should not establish which employees violated the law. In general, an investigation plan should encompass matters such as the goals of the investigation, the scope of the investigation, the team members’ roles and tasks, the timeframe, and the course of action.
Sample Prep Question

3. Which of the following is NOT correct with regard to fraud response plans?

A. A fraud response plan should be complex and extremely detailed to ensure its effectiveness.
B. A fraud response plan can send a message that management takes fraud seriously.
C. A fraud response plan should be flexible and allow appropriate responses based on the particular event.
D. A fraud response plan enables management to respond to suspected incidents of fraud in a consistent manner.
Correct Answer: A

- A response plan will allow management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner. By having a response plan in place, management will send a message that it takes fraud seriously.

- 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 administer. While the appropriate response will vary based on the event, management should include a range of scenarios in the response plan.
Investigation

Digital Forensics
Digital Forensics

- Deleted files and other data that has not been overwritten
- Temporary auto-save files
- Print-spool files
- Websites visited, even where the browser history and cache have been deleted
- Communications sent via chat or IM
- Financial-based Internet transactions
- Documents, letters, and images created, modified, or accessed on the computer
- The time and date information about files
Digital Forensics

- Digital evidence is more volatile than paper information; therefore, it can be easily altered or destroyed.
- Integrity must be preserved.
- If files are destroyed, it can give rise to a claim of *spoliation of evidence*.
- If authenticity is not supported or proven, evidence will be inadmissible.
- Rules are the same.
Locating Evidence

- User-Created Files
- User-Protected Files
  - Camouflaged files
  - **Steganography**
  - Encryption
- Detection Methods
  - Visual anomalies in jpeg, bmp, gif files
  - Audible anomalies in wav, mp3, mpeg files
  - Statistical properties of files deviate from norm
  - Structural oddities suggest manipulation (e.g., size, date, time differences)
Steganography

- Image of a tree with a steganographically hidden image. The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization. The hidden image is shown to the right.
Computer-Created Files

- **Metadata**
  - Data about data

- **Registry**

- **Event logs**
  - System logs record events on the operating system

- **Internet activity**
Digital Evidence
What does 12 terabytes-worth of information look like?

www.neatorama.com/2008/07/08/terabyte/
Locating Evidence

- Printers
  - Internal hard drives
- Copiers and Scanners
  - Internal storage
- Fax machines
- Backup storage devices
- Removable storage
- Smartphones
- Cloud environments
Privacy Issues

- Search policy should include *personal electronic devices*:
  - Smartphones
  - USB flash drives
  - MP3 players
  - Laptops
- Written privacy policy
Computer Investigation and Digital Forensics

- Digital forensics typically involve these phases:
  - Seizing
  - Imaging
  - Analyzing
  - Reporting and testifying
Considerations When Seizing Evidence

- Be certain to document the scene with photographs or a diagram, depending on the complexity of the setup. Remember that it might be a year or longer before testimony about what the office looked like on the day of the seizure will be asked for in a legal proceeding.
Identifying Digital Evidence

- View of server’s wires
- Another reason to photograph the scene
Considerations When Seizing Evidence

- Many people write down or record their passwords near their computers. Fraud examiners should look around for notes that may appear to be passwords. This practice may aid in the discovery of passwords needed to access encrypted data in the event that the subject of the investigation is being uncooperative.
Collecting Volatile Data

- If the computer is off, leave it off.
- Collect volatile data “live” if required.
- Some data may be lost if the machine is shut down.
- Data can be collected while the machine is still on.
Secure the Evidence

- Don’t shut down the system using normal shutdown routines.
- Two “Golden Rules” should be followed. The primary rule is: “If the computer is off, don’t turn it on.”
- The second Golden Rule is: “Don’t peek through the files.”
Imaging

- Image acquisition involves using a standalone hard drive duplicator or similar device to duplicate a computer’s entire drive without altering it.
- This process is known as *imaging* because it takes a hard drive and images it to another hard disk drive or other media.
Analyzing

- Best to use a combination of various forensic tools during the analysis phase.
- Fraud examiners should look for inculpatory evidence (i.e., evidence that serves to incriminate the subject of the investigation) and exculpatory evidence (i.e., evidence that serves to disprove the subject’s involvement in the misconduct).
- Primary concern is to maintain the integrity of the data at all times.
Imaging/Analyzing

MAC Times
Challenges of Cloud Forensics

- Lack of frameworks and specialist tools
- Lack of information accessibility
- Lack of data control
- Jurisdiction of storage
- Electronic discovery
- Preserving chain of custody
- Resource sharing
- Lack of knowledge
Sample Prep Question

1. Often, it is necessary to examine printers as well as computers for data because printers may contain large _______________ designed to do away with the need to have a large print server.

A. Cartridges
B. Hard drives
C. Network connections
D. Phone connections
Correct Answer: B

- Printer technology is another area where it is necessary to stay current on advancing technologies. Many computer networks today have installed printers with large hard drives designed to do away with the need to have a large print server. The printers themselves may now be the repository of additional evidence that at one time resided on a local machine or on a print server.
Sample Prep Question

2. Turning on a computer has little effect on the files contained on the computer system.

A. True
B. False
Correct Answer: B

- Fraud examiners should be aware that files on a computer can be altered simply through the normal start-up process. Most of the Microsoft operating systems, such as Windows XP, change the time and date stamps on a number of files during start-up and delete a number of temporary files during the shutdown process. These pieces of information could be critical to the investigation.
Sample Prep Question

3. Which of the following is TRUE regarding the types of information that computer forensic experts typically can recover from computer systems?

A. Computer forensics specialists can recover information about websites visited
B. Computer forensics specialists can recover time and date information about files
C. Computer forensics specialists can recover deleted emails, link files, and documents
D. All of the above
Correct Answer: D

- Computer forensics specialists can recover, among other things, the following types of information from computers:
  - Deleted files and other data that has not been overwritten (e.g., deleted documents, images, link or shortcut files, and email messages)
  - Temporary auto-save files
  - Print-spool files
  - Websites visited, even where the browser history and cache have been deleted
  - Communications sent via chat or instant messenger
  - Financial-based Internet transactions
4. Steganography refers to procedures used to convert information using an algorithm (called a cipher) that makes the information unreadable.

A. True  
B. False
Correct Answer: B

- **Encryption** refers to procedures used to convert information using an algorithm (called a cipher) that makes the information unreadable.
- **Steganography** is the process of hiding one piece of information within an apparently innocent file. For example, a user can use the least significant bits of a bitmap image to hide a message. By hiding the message in the least significant bits of an image, there is almost no perceivable change in the bitmap image itself. And without directly comparing the altered image to the original, it is practically impossible to tell that the image was altered.
Investigation

Report Writing
Characteristics of a Good Report

- A well-written report contains the following four characteristics:
  - Accuracy
    - Use memorandum that documents the details of the interview.
  - Clarity
    - Avoid using jargon and technical terms; explain terms if used.
  - Impartiality / Relevance
    - Report all facts without bias; include relevant info.
  - Timeliness
Reporting Mistakes

- **Conclusions**—based upon observations of the evidence
- **Opinions**—interpretation of facts
- Be cautious about drawing conclusions
- Conclusions should be _self-evident_ and not necessarily pointed out in the report
  - If not obvious, clarify report
Opinions

- Do not express an opinion on legal guilt or innocence.
- No opinion about integrity or veracity of witness in report.
- Opinions on technical matters permitted if fraud examiner is an expert in the matter.

Examples:

- Permissible expert opinion might be in regard to the relative adequacy of an entity’s internal controls.
- Another might discuss whether financial transactions conform to generally accepted accounting principles.
Reporting Mistakes (Cont.)

- Copy Documents—attach copies of pertinent documents
- Organization
  - Can be presented in chronological order or by transaction
- Analyze the Reader
  - Company insiders
  - Attorneys
  - Defendants and witnesses
  - Media outlets
  - Judges or juries
Report Structure

- Generally, the following sections should be included in fraud examination reports:
  - Background
  - Executive summary
  - Scope
  - Approach
  - Findings
  - Summary
  - Impact
  - Follow-up/recommendations
Reporting Documents

- There are a number of basic reporting documents, including:
  - Memoranda
  - Cover page
  - Exhibits, documents, or enclosures
  - Forms
  - Indexes
  - Transmittal letter
Presenting the Case

- Generally, don’t approach prosecutor until case is complete.
- Must have case ready to present in organized, clear package.
- Chances increased if:
  - Legal, binding admission of guilt
  - Make themselves available to prosecutor
  - Follow up regularly
- If possible, try and approach someone who has a successful track record in white-collar cases and is a hard worker.
Sample Prep Question

1. If, during a fraud examination, a Certified Fraud Examiner obtains a written admission of guilt from the suspect, it is permissible to indicate in the written report that the suspect is guilty of the allegations.

A. True
B. False
Correct Answer: B

- Except for expert opinions, no opinions of any kind should be included in the report. An opinion on the guilt or innocence of a suspect should not be rendered. In the event that the fraud examiner has obtained a confession from the suspect, the confession will speak for itself.
Sample Prep Question

2. When crafting a fraud examination report, CFEs generally should NOT include their opinions regarding the credibility of witnesses.

A. True
B. False
Correct Answer: A

- When crafting a written report, the fraud examiner should be careful not to include any statement of opinion as to the integrity or veracity of any witness, even if the fraud examiner is convinced that the witness is being untruthful. Truthfulness, or lack thereof, can be demonstrated through conflicting statements by the witness or suspect.
Sample Prep Question

3. Which of the following practices will likely enhance the chances of getting a prosecutor to pursue a criminal action against a fraud suspect?

A. Presenting a completed and organized case to the prosecutor
B. Obtaining a legal and binding admission of guilt before submitting the case
C. Following up regularly with the prosecutor
D. All of the above
Correct Answer: D

- Fraud examiners can enhance their chances of prosecution if:
  - They have obtained a legal and binding admission of guilt.
  - They obtain a commitment from the outset for the lawyer to “consider prosecution” based on the evidence obtained.
  - They pledge to help the prosecutor during the trial process.
  - They follow up regularly with the prosecutor to ensure their case does not get forgotten or overlooked.
  - They seek out a prosecutor with a successful track record in white-collar cases and a reputation as a hard worker.