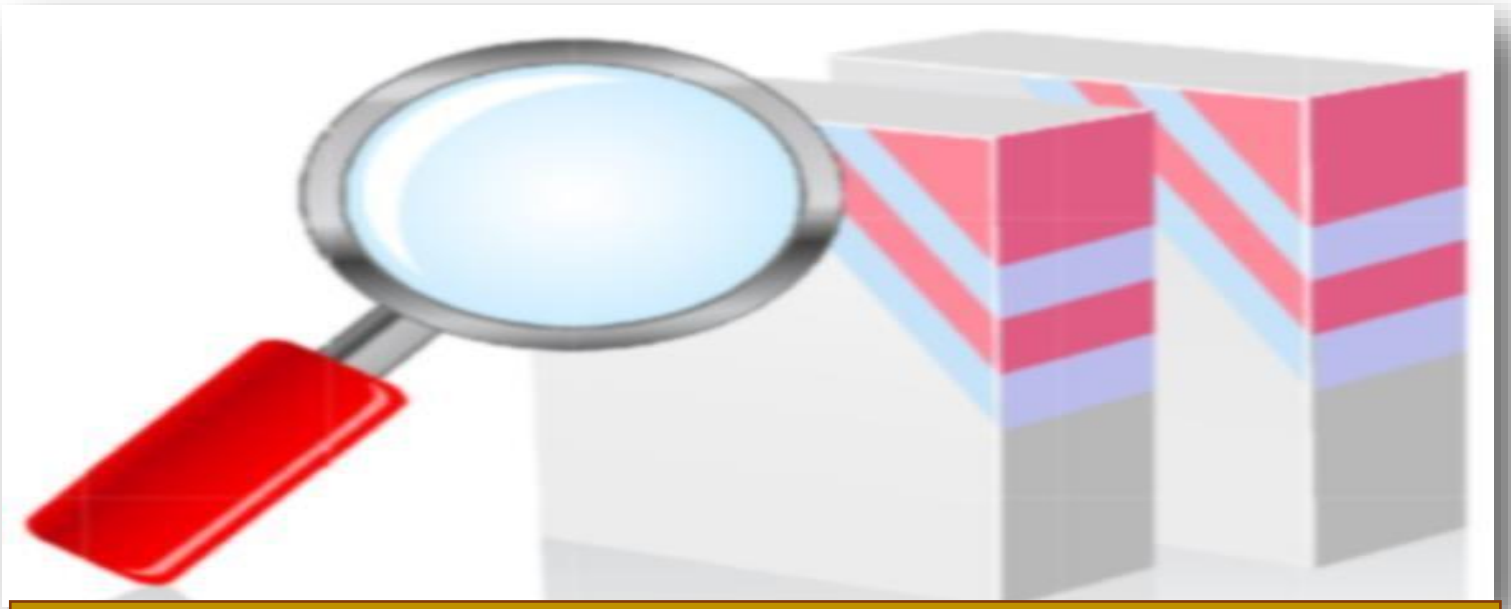


Evidence Gathering Procedures

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Explore different types of evidence.
- ✓ Discuss important steps involved in evidence collection
- ✓ Identify document gathering procedures.

Evidence Gathering

Forensic accountants is a time- and effort-consuming task, but it provides vital support for any investigation. This unit explains what constitutes evidence and outlines the different tools used to collect it.

Evidence

Evidence determines whether an allegation is proved or disproved. For example, if a forensic accountant receives a bank statement showing that the suspect's bank account has increased significantly in the last few months, this will constitute evidence indicating that the suspect may have been involved in a profitable activity. In other words, such evidence may reinforce allegations of fraud. Evidence should be admissible in a court of law as it proves or supports a fact. Proof is different from evidence because evidence results in the emergence of proof.

Direct evidence is evidence that proves a fact without making any inferences or presumptions. In short, those who have direct knowledge (i.e. they have heard it, seen it, or were directly involved in it) of the fact swear of its existence. This may take the form of confessions obtained in a court of law or during the course of investigation.

Circumstantial evidence is evidence that proves a fact through inferences or presumptions. It means having to prove several supporting facts and then analyzing them in relation to one another in order to prove that the ultimate fact in question exists. Circumstantial evidence is admissible in a court of law. Proving the suspect's wilful intent can be categorized as circumstantial evidence. This kind of evidence is normally used for crimes involving malice, motive, intent, etc., or more simply put, to prove something that exists in the mind of the perpetrator. It is usually considered to be as important as direct evidence and its significance may sometimes even outweigh that of conflicting direct evidence.

Evidence is also categorized as oral, documentary, and real.

Oral evidence involves witness accounts and presentation during submission of records and physical objects. Witness testimony includes oral statements by the witness delivered under oath.

Documentaryevidence includes written material such as judicial records, official documents, contracts, deeds, letters, memoranda, private diaries, maps, photographs, diagrams, and any other official or private writing.

Real or physical evidence consists of tangible objects or property. It may include a knife, pistol, or any other weapon. It must be relevant to the case and admissible in a court of law.

Relevancy

This refers to the evidence being of some relevance to the fact. This link should be traceable and significant. Evidence will be relevant if it is a link in a long chain of evidence, or if it is circumstantial evidence that proves that a fact did, or did not, exist.

It is important that investigators only collect facts that are relevant to the case, as irrelevant evidence will not be admissible in a court of law. However, they must ensure that no fact or evidence is omitted simply because there is doubt regarding its significance or relevance. It is at the judge's discretion to determine the relevancy of evidence to the case as there are no set standards for relevancy, which differs from case to case and from one judge to another. Moreover, the investigators should not omit a fact simply because they believe it is non-material or incompetent.

Materiality

Evidence is said to be material if it is significant to the outcome of a trial, or if it determines the guilt or innocence of the suspect. This definition is quite similar to that of relevancy.

Competency

This refers to the admissibility of evidence in a court of law, since evidence should not only be relevant and of material value but should also be sufficiently competent to have legitimacy. Competent evidence includes documents and all other forms of evidence that came from a proper source and were obtained in a legal manner. Evidence may be relevant and material but incompetent at the same time if it is inadmissible, such as hearsay.

Hearsay

Hearsay refers to evidence that was not in the personal knowledge of a witness; It may be simply something he/she heard others say or a document that was prepared by others and not the witness. It is also called second-hand evidence and it is not admissible in court. For example, if an investigator alleges that corporate cheques to payees were for the personal expenses of the subject, this is categorized as hearsay and not actual evidence. The nature of the payments should be proved through third-party testimonies, or the subject's own records. Cross-examination is a crucial tool in order to determine the authenticity of facts, as it tests the credibility of the witness and the witness's observations and memory and identifies any prejudices or errors. It may clarify whether the witness is committing perjury by deliberately altering facts, or whether there were any unintentional misstatements.

Admissions and Confessions

An admission is a statement or an act of the accused that might be offered as evidence against him/her. It is not the same as hearsay. It may also involve a prior written or oral statement, or a prior act that is inconsistent with a person's pleading or his/her position at the trial. Admissions can be used both as evidence and as means to discredit a person as a witness. Therefore, a confession, which is a statement by a person that he/she is guilty of a crime, can only be used as a fact and not as opinion or hearsay.

Proving Cases through Documentary Evidence

The type of evidence is what differentiates financial crimes from non-financial crimes. In cases of murder or burglary, for example, evidence usually comprises fingerprints, weapons, and other physical or real objects. Sometimes, documentary proof and photographs are also considered important evidence but these are relatively rare in non-financial crimes. Financial crimes, on the other hand, are highly document-based. Investigators are usually faced with volumes of documents, receipts, papers, etc. What is considered an unusually high volume of evidence for non-financial crimes is a very common volume for financial crimes.

In this unit, we will begin with the basics of document collection. We will discuss the various methods of collecting documents, such as obtaining subpoenas, search warrants, consensual searches, etc. Moreover, we will include various tips and tactics on the types of documents that a forensic accountant may come across during the investigation.

It is imperative to organize and collate evidence carefully in order to avoid the chaos ensuing from the sheer number of documents that a forensic accountant has to deal with. The next section provides a framework for creating a tracking system for the evidence; this will be useful regardless of the size of the investigation and the volume of evidence.

The last section deals with methods of proving a case. We discuss how forensic accountants might use organizational techniques together with logic and inference to prove their case. It is important that forensic accountants have a thorough understanding of the legal process involved in proving their case before they master the art of using the evidence they have gathered to establish guilt.

Gathering Evidence

Forensic accounting investigations are based on gathering, documenting and retaining evidence. The decisions that a forensic accountant takes during the course of gathering evidence are closely associated with the scope and manner of the investigation. The ultimate value of the conclusions drawn from the investigation depend on the credibility of evidence; therefore, it is important that evidence is gathered, preserved and stored in a proper manner.

Documentary evidence involved in forensic accounting investigations can be classified as electronic documents or media, and physical or paper documents. Sometimes a document can exist in both electronic and paper formats, for example when an electronic document was printed out and modified by the recipient through notations on the printed version. Another common yet crucial form of evidence is the testimonial evidence of the people related to the investigation. Testimony usually comprises people's oral narrations given to the investigators based on their memory, or their interpretations of documents that contain information pertaining to the investigation. Techniques related to gathering testimonial evidence differ from those used to gather electronic or physical documentary evidence.

Forensic accountants create documents during the course of the investigation in addition to the documentary evidence that already exists in the form of transactions, receipts, etc. These documents

can be regarded as evidence and can be presented to the court or to the regulators in charge of regulating matters associated with the investigation. Just like other evidence, such as business records, these documents should also be preserved and maintained properly.

Critical Steps in Gathering Evidence

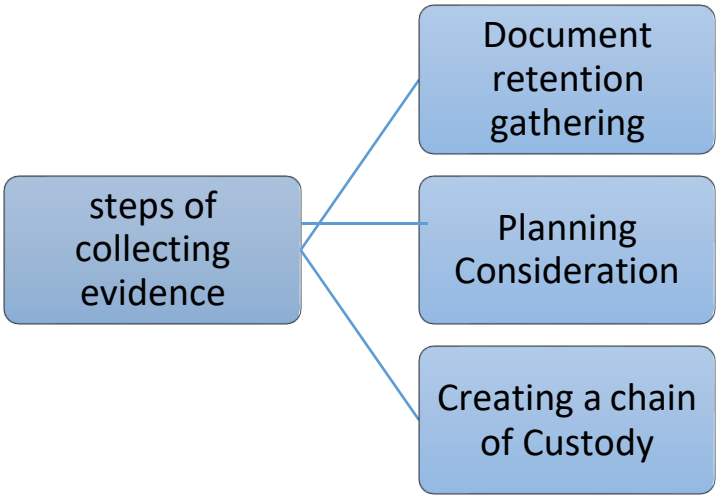


Fig 1.1

Document Retention Considerations

Considering forensic accounting investigations' heavy reliance on documentary proof, document retention and preservation are tasks of the utmost importance. Many points must be borne in mind, and it is advisable to hire a counsel to discuss the complications.

It is important to preserve electronic evidence present in the company's accounting system because during the course of business it is common for transactions to take place, assets to be acquired and sold, accounting systems to be modified, new information to become available, and estimates to be revised. It is better to establish some basic points at the beginning of the investigation. For example, will the forensic accountant be responsible for retaining records? Which documents should be retained as evidence, and for how long? This can be a complex area; therefore counsel should be consulted to ensure that the firm's policies as well as accounting regulations and laws are being conformed with. Moreover, a huge volume of files and documents will be reviewed during the investigation; therefore, investigators must decide which, out of all these documents, should be retained. There are certain circumstances, however, that require all documents and electronic files to be retained. For example, subpoenas may require all information to be presented.

Planning Considerations

It is usually important to meet up with clients, depending on the nature of the investigation, in order to discuss the type of evidence that may be required and to locate the evidence relating to the time period under scrutiny. As business structures and data processing operations of companies change over time, these meetings held to discuss financial accounting records become all the more important. Suppose, for example, that the investigators need to review certain employees' e-mails over the past two years but find out that the company's back-up data cannot be located and that the e-mail server only stores data for up to 60 days. In this case, it would have been helpful to tell the client that this kind of data may be required; they might then have arranged access to it or told the investigators that it would not be available.

- Prior planning requires the following:
- Reviewing the client's policies on record retention and ensuring compliance.
- Visiting storage locations for paper records off and on site.
- Reviewing the technology used for transaction records, such as customer and vendor invoices, contracts, etc.
- Ensuring the existence and storage of employee files.
- Checking whether there are any files at the employees' homes or in their personal computers.
- Checking the file retention practices at various corporate locations, as they may differ significantly from one location to another.
- Analyzing the organizational hierarchy and knowing who reports to whom.
- Checking the medium of storage for computerized records on and off site.
- Reviewing the company's back-up procedures that are used for employees' computers and e-mails, knowing when back-ups occur, how much information is lost and how much is retained, and which information is retained on servers and which on individual hard drives.
- Checking whether any records are retained by or about former employees of the organization.
- Analyzing system changes that have occurred in the company's accounting systems or e-mail systems.
- Reviewing documents related to corporate functions that have been outsourced, such as payroll and internal audit.
- Creating a written plan for the collection of documents in order to give the investigation a clear direction and focus.

A plan will indicate the scope of the investigation and be a helpful tool to prove that the documents sought were relevant to the investigation. It will also avoid unnecessary hoarding of information, which may include different types of documents, from various witnesses, stored at different locations.

Although in some situations the forensic accountant might purposefully adopt an approach where volumes of evidence are collected and stored in different locations, generally a more focused approach is preferred.

Forensic accountants hardly ever receive all the information they have requested without hurdles. Sometimes, fraudsters use these hurdles, such as confusing accounting and financial terminology, to confuse investigators and conceal their fraud. A plan helps to minimize the confusion created by perplexing terminology. Take, for instance, an Aged Trial Balance of Accounts Receivable requested by the investigator.

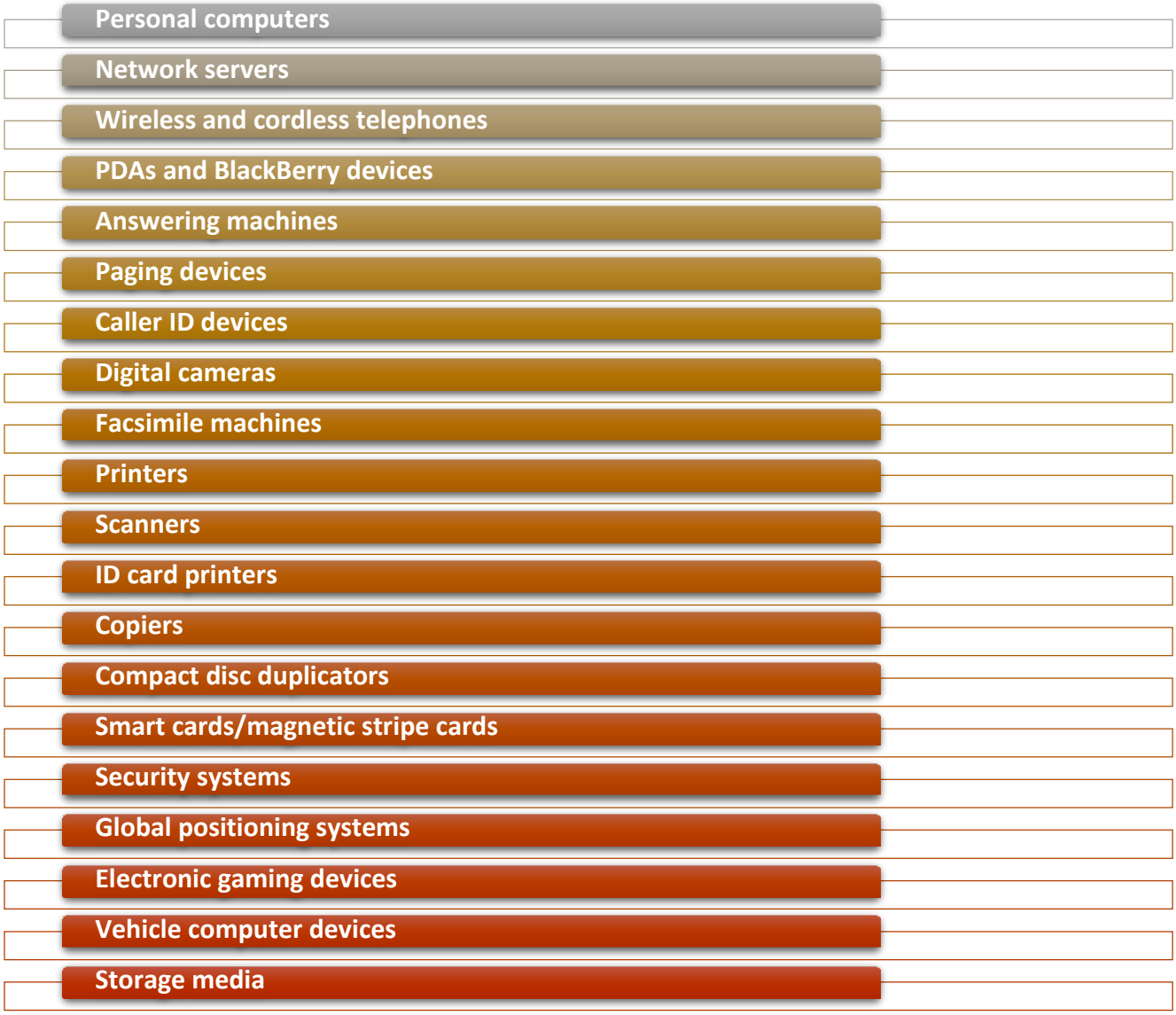
The company responds that such an account does not exist (which is highly improbable because it is a customary accounting document). As it turns out, the company does maintain such an account, albeit under a different name, Listing of Open Receivables. When the culpable party is confronted, they say that they were not trying to conceal the document but simply did not recognize the different name used for it. In order to avoid giving suspects such opportunities to create confusion, it is advisable to make a

list of all user reports with their exact names, users' names, and when the reports were developed and distributed.

Creating a Chain of Custody

The chain of custody serves as proof that the evidence has been properly preserved from alteration and damage from the time when it was collected to its presentation. It signifies to the court or regulatory body in front of which the evidence is being presented that it has probative value. Therefore, the investigator should discuss the level of detailed record-keeping required to establish a chain of custody with counsel and the client before gathering the evidence.

The following gadgets and devices usually contain relevant data:



As technology becomes more advanced and keeping up with it requires expert help, the best practices used for collecting electronic information also continue to evolve. The investigative team cannot be efficient without possessing or having access to the requisite IT skills in order to identify, gather and, more importantly, assess the integrity of electronic information.

Evidence Created by the Forensic Accounting Investigator

Working Papers

A forensic accountant produces summaries and analyses of factual material, which are usually the basis of testimony in cases of litigation to recover losses if shareholders commence litigation against the

enterprise, i.e. class-action lawsuits, or if the forensic accountant is required by law to produce them in front of regulatory bodies.

The kind of material and documents included in the working papers differs from one investigation to another, depending on the nature of the investigation. The following is a list of typical documents that comprise working papers:

- *Accounting records and other documents.* This category includes all possible accounting records such as general ledgers, sub-ledgers, financial management reports, reconciliations, journal entries, internal audit reports, purchase orders, vendor information, accounting journals, management reports, contracts, telephone, computer system and security system records, desk files, e-mails, websites, and any other accounting record or document.
- *Public record searches.* The information gathered through public record searches can be diverse and may include newspaper articles, hobbies and interests, investments, philanthropic work, online chat room discussions, etc.
- *Electronic computer files.* These includee-mails (forwarded e-mails, senders, recipients, etc.), computer files, any data stored in handheld digital recorders, etc.
- *Photographs or digital photos, preferably with a date/time stamp.*
- *Documentation specifying chain of custody.*
- *Interview notes and audio recordings.* These are notes taken by the investigation team during interviews conducted with witnesses, suspects and other personnel.
- *Third-party information.* This is information or data provided by interested third parties such as counsel, external auditors, etc. This information may be in the form of audit reports, management letters, bank statements, cancelled cheques, bank advice, or any other banking documents, records related to non-audit services, documents acquired through warrants or subpoenas, etc.
- *Court pleadings and deposition transcripts.*

What Kind of Evidence should be Gathered?

There are hard and fast rules regarding the kind of documents that should be retained as evidence. However, certain documents may be useful as evidence in a variety of investigations.

Investigations of Vendors

These should be centred on all information relevant to the disbursement of money to vendors; i.e. where did the money go, and for what purpose was it used? This information includes the following:

Information about the vendor stored in the company's master file data for accounts payable.

Contracts, purchase orders, invoices, and documents used to obtain payment approvals, receiving documents, correspondence concerning credits, billing errors, etc.

Results of the public record searches used to qualify a vendor and internal feedback regarding vendor quality. Data mining for similar names, duplicate addresses, duplicate payments, purchase orders, invoices, etc. may be used to collect such documents. In addition to computer forensic techniques, interviews and public record searches regarding the vendor may also be useful.

Investigations of the Foreign Corrupt Practices Act Violations

These usually concern disbursements and focus on the interviewing technique. Let us suppose that the government awarded a contract involving large disbursements of payments to a company through a middleman who was working as a consultant as per company records. The forensic accountants were unable to find a fair exchange for the payments that were being made, according to their judgement. Investigating such a case would require extensive collection of documents and interviews regarding the exact purpose of every payment.

Investigations of Improper Related-Party Activity

These require documents concerning the nature of the relationship between the parties involved in the transactions. These documents include interview notes, internal control policies, e-mails, public record searches, and any other documents useful in the analysis of fair value economic exchange.

Investigations of Employee Misappropriations

These are usually focused on the documents that were being handled by the employee in question. They include desk files, computer data, e-mails, records of the employee's access to corporate computer systems, records of the employee's access to the company's facilities, security camera tapes, payroll records, employment records, interview notes, etc.; in addition to official files and documents, the employee's personal lifestyle and property ownership may also be relevant. Cell phones and personal computers belonging to the employee may contain important information about the employee's activities.

Investigations of Specific Allegations

There may be various sources triggering investigations of specific allegations, such as anonymous letters, hotlines, anonymous tips, and exit interviews. The investigation plan for gathering relevant evidence depends on the nature of the allegations. Generally, however, investigation plans begin broadly, in a non-specific manner. It is always useful to take all allegations and tips seriously, although some are just unfounded allegations by disgruntled employees. Being thorough with regard to anonymous tips and allegations gives external auditors and regulators the impression that the investigation team is addressing the matter seriously. This may also lend credibility to the conclusions of the investigation team.

Investigations of Financial Statement Errors

These require access to and a review of all reports, statements and documents involved in the company's financial accounting transactions and business records, employee files, and e-mails of all

parties involved in the transactions. Such investigations involve approaching and interviewing third parties such as banks, former employees, vendors, and customers for evidence of transactions. Sometimes it is helpful to copy the entire general ledger and e-mail servers to another data centre location in order to preserve the evidence until the investigation team is ready to review it.

Document Collection

"Best evidence" does not refer to the most appropriate evidence to support a claim; it simply means that all evidence submitted must be original. All cases require best evidence to be submitted.

In the event of original evidence being unavailable, investigators should clarify the reasons for its unavailability and prove the accuracy of the copy that is being submitted. Although there may be some exceptions to this rule, it is generally considered inflexible.

Financial crime investigators should attach special importance to this rule. For example, when non-financial crime investigators are trying to prove that "A" shot and killed "B", they usually need the gun used in this murder as evidence. However, when financial crime investigators are trying to prove that CFO "X" embezzled money from the company's pension fund, copies of bank statements incriminating "X" may hold weight with the prosecutors. Although this may be admissible as evidence in court, the original documents and bank statements will be required.

The investigator's primary responsibility should be to preserve and safeguard all relevant documents. Regardless of how documentary evidence was gathered, the investigator has ultimate responsibility for its safekeeping and production once it is in his/her possession.

If the investigator is well aware of the precautionary measures and protocol required for handling evidence, this responsibility is not too difficult to fulfil.

Types of Documents to Expect

- *Signed statements.* It is always useful to obtain written and signed statements from witnesses as well as the complainants. Although these statements will not be substitutes for the actual testimonies offered by witnesses in court, they may provide a summary or an outline of what might be expected at their trial testimony.

- *Transactional paperwork.* Every business operates in a different manner, and while the basic documents will be generally similar, there will be some differences. This is where pre-planning will be useful for the investigators. Therefore, they must always be on the look out for any documents or paper trails left by transactions such as invoices, vouchers, original records, etc. that may indicate the flow of money.

- *Intranet sources.* More and more businesses are creating networks connecting their employees and departments. This intranet connection not only increases productivity but also serves as a

source of valuable information. Investigators need to examine chat facilities and weblogs where suspects and witnesses are most likely to be found. Although they will find no transactional information there, they will be quite likely to spot unofficial communication of value to the investigation. This communication may include gossip, rumours, and crucial background information related to employees and managers.

- *E-mails.* E-mails are a very common mode of communication in a business organization, and the investigators might benefit from this when they are looking for evidence. Not everyone is careful about what is sent in an e-mail and to whom. Most messages are saved on the corporate server for a long time, which is helpful for investigators seeking to examine messages sent through e-mails.

The list above mentions sources of information that may represent a good place in which to begin the investigation. Planning the investigation and obtaining background information beforehand may clearly define what the investigators are looking for. Moreover, the investigators should be flexible in their technique and should be able to tailor their searches according to circumstances. For instance, perhaps the suspect does not communicate through e-mail at all and prefers to use paper memos. In this case the investigator should be able to search through the paper trail for evidence or crucial information.

Sources of Documents

Documentary evidence may be present in multiple locations, but they can be divided into three broad categories:

(i) Whether it is a pensioner swindled out of his/her pension, or a large multinational corporation that has lost millions to a fraud, the victim of the financial crime is the first place where investigators should look;
(ii) the next source is the third parties who may have access to or possess documentary evidence;
(iii) lastly, the investigators should look for evidence possessed by the suspect.

It is advisable to follow the above order, although where and from whom the investigators find evidence first will differ depending on the nature of the case and the business.

Documents from the Victim

Investigators should start collecting documents as soon as they receive a complaint or an allegation. Usually, the victim of a financial crime will have some documentary evidence to support his/her allegations. It is advisable to collect those documents rather than telling the victims to wait until the investigators have looked into the allegations and made a case.

If the investigators do not collect the victim's documents, there is a chance that they will be lost or destroyed. Sometimes the party who files a complaint is complicit in the crime but reports the crime regardless, possibly to divert suspicion from the reporting party. Therefore, if the investigators allow some documentary evidence to remain with the reporting party, the latter may destroy those documents. Even if the reporting party is not involved in the crime, there is every possibility of the suspect or his/her accomplices gaining access to the documents and altering, stealing or destroying them.

If the victim is reluctant to give the documents to the investigators, as is the case with sensitive financial documents, they should make copies or issue receipts. It is important to tell the complainant about the need for proper procedures to safeguard documentary evidence and ensure that it is admissible in court. The investigators should try to persuade the complainant that evidence would be safer with them as they are trained to handle sensitive documents. Thus, the complainants would retain copies of the original documents along with the itemized receipts for everything collected from them by the investigators.

Investigators should be meticulous in their paperwork, as their liability insurance will only protect them to a certain extent. When faced with hundreds of documents, some investigators may be tempted to lump them all together in bulk and list the groups of documents. This may cause problems when it becomes difficult to locate a specific document. Moreover, investigators may be held liable if the victim claims that he/she disclosed sensitive financial information or a trade secret and the investigators cannot disprove it. Therefore, it is always helpful to list everything even though this may be time-consuming.

Even when complainants have no documentary evidence to substantiate their allegations, the investigators should still record a written and signed statement. This statement would serve as proof that a complaint had been made should, for whatever reason, the complainant recant the statement in the future. There is also a possibility of the original witness or complainant becoming unavailable in the future. In this case, a written statement would serve as a reference in the witness's absence, although it would not be admissible in court. Should the witness change his/her original statement or forget important details, the written statement would obviate the need for the investigators to start from scratch.

Documents from Third Parties

Usually, in financial crime investigations most of the documentary evidence is collected from third parties. A criminal must act like any other person, have frequent interaction with other businesses, deposit money in banks, and seek advice from financial and legal experts, etc. in order to succeed as a financial criminal. Therefore it is very likely that third parties such as banks, business organizations, and the government will possess crucial pieces of information that link the suspect to criminal activities.

Due to the diverse nature of a business, its particular pattern of activity, and its circle of influence, there may be various sources of information. The level of diversity of a business will determine where

incriminating documents might be found. Sometimes a business's circle of influence extends only to financial professionals, whereas other businesses may have extended their influence beyond the financial sector into the community.

A suspect's contacts can generally be broken down into five categories. Firstly, there is the financial sector, which includes banks, insurance professionals, and brokerage houses. The suspect will definitely have interactions and contacts with the financial sector. Secondly, the financial criminal is likely to have interactions with professionals such as lawyers and accountants. Thirdly, there are interactions within the industry with business organizations, networking groups, and associations. Fourthly, there is the government. Lastly, the financial criminal will have personal contacts who may not be involved in illegal activities but may nevertheless possess important information.

Financial Contacts

Almost all criminals will have some form of contact with a financial institution such as a bank. Therefore, banks are good places to start a search for information. Investigators may gain access to crucial information through paper trails left by the criminal's interaction with the bank.

It is possible that civil, local and state criminal investigators will not have access to documents protected under federal law such as the Bank Secrecy Act. However, there are several bank statements and bank-related documents that might be accessed through civil summons and pre-trial discovery tools. Local and state law enforcement investigators might also gain access to the majority of the documents simply through search warrants and grand jury subpoenas.

Sometimes, inexperienced investigators tend to take bank documents at face value and do not look beyond the values recorded on bank documents regarding income or payments to business associates. It is important to look for non-obvious clues in bank records. Bank records contain much more information than the usual cash flows, such as metadata. Metadata, simply defined, are data that describe data. The metadata of a bank record would be the information related to the transaction shown in it. This information includes date, time, teller information, origin, and format of the transaction. Investigators may find numerous clues in metadata.

Digital or manual analysis of metadata contained in all transactions may reveal the patterns of activity and give direction to the investigation. Once these patterns are revealed, the investigator may be in a position to make predictions about future illegal activities and may be directed towards other associates or assets.

Each transaction generates metadata that provide a complete picture of the suspect's movements. Every cheque collects clues, in addition to the American Banking Association's routing numbers, as it goes through the clearing process. For example, a teller stamps the cheque with a unique transaction code, time, date, and teller's information during an over- the-counter transaction. Therefore, each transaction becomes identifiable with a unique code and can be linked to a particular time. In the case of deposits, the source of funds is also traceable. Exhibit 10.1 is an illustration of metadata. Here, it is important to remember that there are two general categories of transactions. The first category includes transactions

related to the account holder, such as deposits, withdrawals, and debit/credit memos. These are called flow-through transactions. The second category includes all other transactions, which are called non-account transactions because they are not directly related to the account holder. Loans, CD transactions, third party transactions, and safety deposit transactions are common examples of non-account transactions. Every transaction has a set pattern more or less.

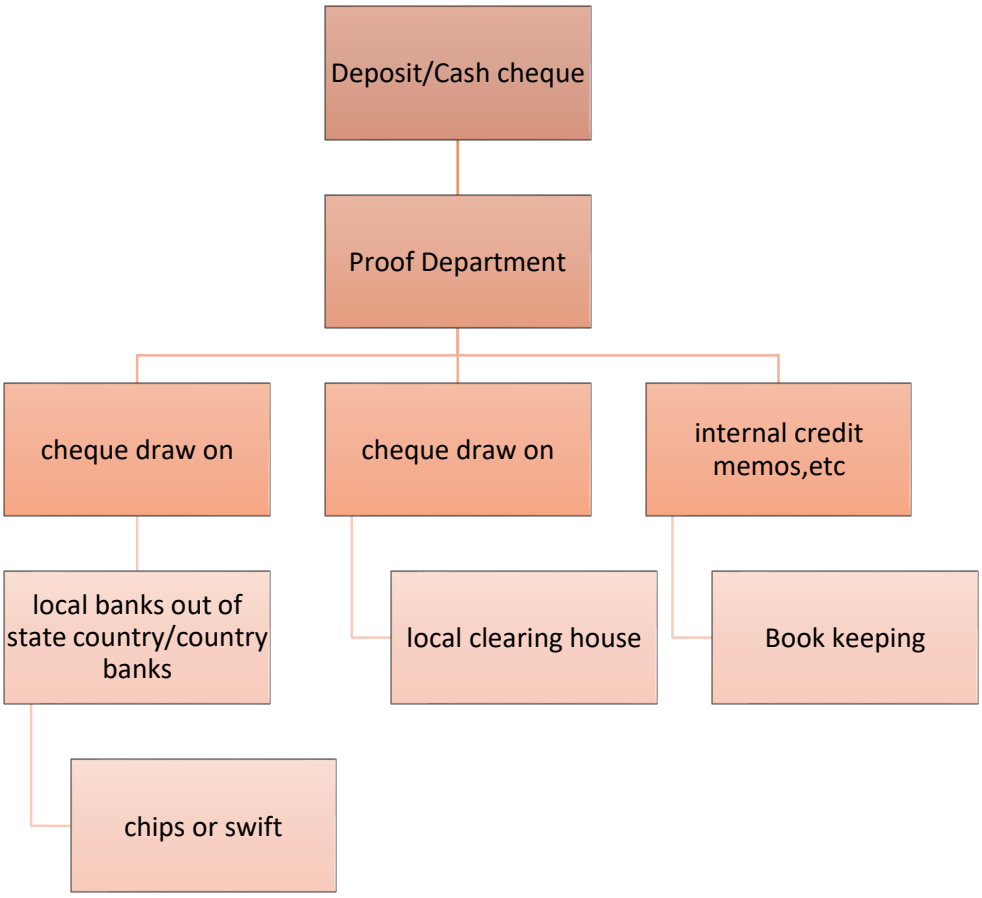
Every transaction has an entry point, be it a window transaction where the suspect wants to make a deposit or presents a draft for withdrawal, or a transaction at the ATM or at a point of sale (POS). Then, the items involved in the transaction move from the entry point to the proof department. Here, the teller's calculations are checked and the items are given a discrete bank identification number and transaction-specific MICR information. Transaction items move to the microfilm department from the proof department where they are recorded and entered into the bank's computer system.

After passing through the microfilm department, transactions are separated by the bank and sent to different departments for clearing. Clearing refers to the money changing hands. This process may become complicated depending on whether the transaction is in-house (the item is presented against the institution against which the claim is held) or an outside transaction. Ultimately, the goal of the clearing process is to ensure that there is an exchange of claims between the payer and the payee. When the transaction is in-house, meaning that the payer and payee are the same, the in-house clearing department receives the transaction data, after which they are sent to the bookkeeping department where customer records are updated.

When a local institution is involved in the transaction, the bank sends the transaction items to the local clearing house. When the payer and payee institution are not the same, and when the parties involved in the transaction are within the same city, the transaction items are sent to the local clearing department. Local cheques are usually cleared through the Clearing House for Interbank Payment Systems (CHIPS) or the Fedwire funds transfer system.

Transactions involving institutions outside the local area have to be processed through alternative means. The transit department is responsible for ensuring the proper clearance of these outside transactions. Most international transactions are dealt with by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and others by Fedwire or CHIPS.

Transaction Flow chart



Professional Contacts

The suspect's accountant may be in possession of the following documents:

- Working papers identifying expenditures, sources of income, loans, and hidden accounts.
- Notes and memoranda that assisted in preparing the suspect's income tax return.
- Copies of income tax returns.
- Minutes of corporate meetings and documents indicating the existence and identity of shell companies.

Most public accountants maintain accounting records meticulously; hence, they are able to provide valuable evidence against the suspect. Therefore, the suspect's accountant might provide any financial document controlled by the suspect.

The investigators might also approach real estate professionals because they maintain records. Title companies and real estate agents possess copies of contracts that can identify real property owned by

the suspect. These agents and companies usually retain copies of settlement sheets, insurance documents, and copies of any other financial document that was used in order to materialize the transaction. Buyer/seller information, price, down payment, and the distribution of money at the time of closing are also shown in the documents. The investigator should be open to the possibility of the real estate agent also acting as a property manager. In a situation where a real estate agent has acted as the suspect's property manager, the agent will also possess copies of leases and tenant information.

Industry Contacts

Investigators might compare suspects with information regarding the industry. Industry-based organizations usually have a vast amount of data about marketing and sales information of the industry. These data may represent a yardstick by which the investigators might measure the timing and amount of cash flows in the suspect's account. While industry data may not always be relevant to the suspect, they do provide valuable information about actual sales and expenses. Take, for example, an association of video retailers. Though they may not be able to provide the specific number of videos rented monthly by the suspect, they do possess the statistics for the industry average. Sometimes the data are relevant to specific regions or cities. The investigators are able to spot irregularities such as overstated revenues in the suspect's accounting records due to this information.

Other than contacts in the industry, suppliers and customs will also have records of their transactions with the suspect. The nature of their relationship with the suspect, the frequency of contact and the level of cooperation by the third party will determine the value of the information to the case.

Government Contacts

Data collection is one of the primary responsibilities of government agencies and regulatory bodies. Some of these data, such as census and accident data, are aggregate while some of them are identifying. An individual may generate a huge amount of data such as birth certificates, death certificates, marriage licenses, and corporate filings; therefore, collection and processing are required by an overseeing authority.

Investigators should begin by scrutinizing the suspect's county records before moving on to business, property, legal and personal records. These records are usually open to public inspection.

- *Business records.* Local businesses are highly regulated. A basic search includes scrutinizing occupational licenses, annual reports, corporate registrations and filings, state licenses such as real estate, mortuary or banking commissions, fictitious name registrations, etc. Other records include warnings for rule violations or failed inspections by regulatory bodies. The investigators must ensure that all entities and organizations with which the suspect is associated are scrutinized. This may be a repetitive process as new names emerge during the course of information gathering.

Property records. Property records may be known by various names depending on the jurisdiction. Some jurisdictions keep recorded deeds and tax assessments in separate files. Both these documents

may indicate nominee ownership of property or a fictitious transfer of property, and they are therefore important. Investigators should focus in particular on quitclaim deeds. These instruments are legitimate and fairly common in real estate but financial criminals may abuse them.

- *Legal records.* The rate at which jurisdictions make their systems and legal records available online depends on the size and budget.
- *Personal records.* Going through the suspect's personal records and ensuring that all of the suspect's identities are accounted for is very important. All typographical errors, birth records, name change petitions, and any other document regarding the suspect's identity may represent a breakthrough in the investigation.

Personal Contacts

Spouses, partners, exes, etc. can be valuable sources of information. While they may not be able to provide documentary evidence, they can be as valuable as interview subjects. Personal contacts usually know the suspect's thoughts and opinions, and may even have some e-mails or any other correspondence that might be used as evidence. Personal contacts may also be able to identify bank accounts.

Documents from the Suspect

Investigators usually target the suspects last when they are gathering evidence. While suspects may not always be the last people from whom documentary evidence is sought, investigators typically exhaust all their options before approaching the suspect. Investigators are advised to familiarize themselves with the suspect's personal and business habits as the lack of such knowledge may cause them to make faulty judgements, miss important evidence, discard valuable evidence as irrelevant, etc. All these scenarios are undesirable.

Once the investigators have decided that they must target the suspect for further evidence, it is important that they bear a few things in mind. The investigators may not possess the necessary tools for gathering information from the suspect. In, for example, a criminal case there is a wide range of options such as search warrants and subpoenas.

On the other hand, options are limited in civil investigations. Investigators are generally limited to the civil process. While, in a criminal case, the investigators might resort to search warrants issued by the court, or a court ordered wiretap, they cannot do so in civil investigations. Most third-party documents are obtained through civil processes; however, documents in possession of the suspect cannot be obtained in that way. There is no guarantee that the suspect or defendant will produce the documentary evidence upon demand or even admit that such documents exist, since the civil process of obtaining evidence takes place on a voluntary basis.

In many cases, the civil process system can only be invoked post-filing. In other words, court jurisdiction is determined only after the suspect becomes the defendant. It is important to consult with the counsel

before initiating anything, regardless of whether the case is civil or criminal. Consensual production of documents is a powerful tool and must not be underestimated.

Document Organization

After discovering the nature of documents and records available, it is important for investigators to know how to organize them. There is always a possibility of information overload as financial crime investigations involve more documentation and greater collection of records than any other type of investigation. This also results in an increased risk of loss or destruction. Therefore, it is all the more important to have an efficient system of organization. There should be a plan for storing documentation long before investigators even start collecting documents and records.

Collection

The evidence present at the scene must be secured and packaged in order to ensure that there no alterations are made and that no damage occurs during transportation. Packaging them in storage boxes and individual envelopes will protect items. A thorough inspection and analysis of the documents cannot be carried out immediately due to lack of time; however, it is important to give them a cursory inspection to ensure that whatever is being seized is included in the warrant authorizing seizure.

Usually, the lengthier an investigation, the less time available to investigators. Therefore, if investigators give in to the temptation to scrutinize evidence on site, the length of the investigation may easily exceed the budgeted time. The search for evidence at the crime scene should focus on the efficient and safe collection of the items authorized in the warrant. Once the search comes to an end, the suspect must be given proper receipts, after which the evidence might be transported back to the office where the investigators can evaluate it thoroughly.

Storage

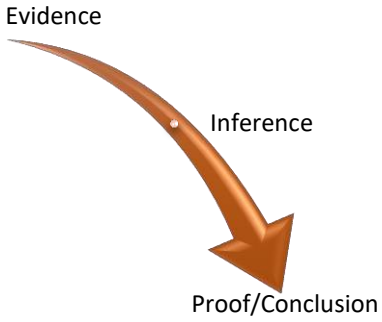
Maintaining the integrity of evidence is crucial for the case. Admissibility of the evidence in court and the issue of civil liability depend on the authenticity of evidence obtained from the defendant. To ensure admissibility and to avoid civil liability, the investigators must store and use the evidence carefully.

Any minor alteration in the evidence may result in the court refusing to admit it. While any marking of the evidence should be avoided, it is important to assign unique numbers to individual items for the purposes of identification and organization.

The Process of Proof

Inferences are the means through which legal cases are proved. They are like chains that form a logical linkbetween point A and point B. The strength or weakness of the case depends on the strength of these inferences. Legally speaking, inference is the persuasive effect of each individual item of evidence.

Jurors may infer that a fact exists when evidentiary items exist. Therefore, proof refers to the net effect of inferences. Simply put, inferences originate from evidence and conclusions are a result of the combined effect of inferences. Legally, conclusions drawn from inferences are said to be proof.



Proof through Inference

Inference can be termed weak or strong depending on how clearly an inference can be drawn from existing evidence. A weak inference suggests that there is a great leap from evidence to conclusion. A shorter distance between evidence and conclusion, or a closer link between the two, means that the inference is strong. The following statement is an example of a weak inference: “the defendant and his ex-wife were not on good terms with each other; therefore, it can be concluded that the defendant killed his ex-wife”. On the other hand, the following statement suggests a strong inferential relationship: “I saw the defendant stab his ex-wife; therefore, it can be concluded that the defendant killed his ex-wife.”

The first statement has too many intervening steps between the evidence and the conclusion whereas the second statement has very few, if any, intervening steps between the evidence and the conclusion. The investigator’s goal should be to minimize the intervening steps between the evidence and the conclusion.

Conclusion

Evidence is meant to prove the case. Whether or not investigators can prove their case depends on how evidence was collected and what was recovered. The logical argument behind the case will dictate whether the jury will reach the same conclusion as the investigators. This unit dealt with the kinds of evidence that investigators may encounter during the course of their investigation. It then discussed practical means of collecting and organizing defensible evidence. Finally, this unit discussed the ways of proving cases through inference and the importance of binding all evidence with a chain of logical inferences.

This unit has thus provided a firm foundation for the process of establishing legal proof.

Further Reading:

- ✓ *Singleton, T., et al (2006) Fraud Auditing and Forensic Accounting*
- ✓ *Albrecht, C.C., Albrecht, W. (2005) Fraud Examination*
- ✓ *Wells, J. T. (2006) Principles of Fraud Examination*
- ✓ *Brown, A., Doig, A., Summers, G., Dobbs, L. (2004) Practically Fraud*