Emergence and Necessity of

Forensic Accounting

SUBMITTED TO

GLS UNIVERSITY

FOR THE DEGREE OF

MASTER OF COMMERCE

FACULTY OF COMMERCE

BY

URVIBEN PURANI

ROLL NO: 77

ENROLLMENT NO: 201900913010074

UNDER THE GUIDANCE OF

DR. GAURANG PRAJAPATI

(FACULTY OF COMMERCE, GLS UNIVERSITY)

FACULTY OF COMMERCE

GLS UNIVERSITY

CERTIFICATE

This is to certify that **MS URVIBEN PURANI** has worked and completed her project work for the degree of MASTER IN COMMERCE at the FACULTY OF COMMERCE in the subject of ACCOUNTANCY on "**Emergence and Necessity of Forensic Accounting**" under my supervision. It is her own work and facts reported by her personal findings and investigations.

Name and Signature of the guide: Date of submission

(Dr Gaurang Prajapati)

Name and signature of professor in charge Stamp of institute of the substitute

DECLARATION BY THE STUDENT

I, the undersigned **Ms. Urviben Purani** hereby, declare that this project work entitled "**Emergence and Necessity of Forensic Accounting"** is a result of my own research work and has not been previously submitted to any other university for any other examination.

I hereby further declare that all the information of this document has been obtained and presented in accordance with the academic rules and ethical conduct.

Roll NO = 77

Year = 2021

Enrollment No = 201900913010074

Date: 14-04-2021

Place: Ahmedabad

Scholar :

Name & Signature:

Urviben Purani

INDEX

1. Introduction

Enron, WorldCom and Tyco names are familiar to us. They are all infamous for same reason: Fraud. According to the recent estimate around $ 3 trillion is lost globally to occupational fraud. Fraud has consequences for economy, corporate and individual.

As described by Howard Silverstone in his book fraud is an opportunistic infection that bursts forth when greed meets the possibility of deception. The scandals like Enron resulted in the loss of public trust and huge amount of money.

Cracking down on fraud is critical for a country that needs investment. In order to avoid fraud and theft, and to restore the badly needed public confidence, several companies took the step to improve the infrastructure of their internal control and accounting system.

Business has changed since the days of Luca Pacioli. It has changed since the advent of computers. Forensic accounting is the field which is called upon to address the issues of prevention and investigation of white-collar crimes. Needless, to mention the case of Harshad Mehta, Hiten Dalal, Mukesh Babu, Ketan Parekh and Ramalingam Raju's Satyam etc. which have put question mark on the efficiency of the existing regulation of Indian financial market. Investigating these frauds can be complex. One needs to perform proper investigation and there comes the term Forensic accounting. Forensic Accounting means performing a Financial Investigation.

Forensic accounting is a rapidly growing area of accounting. It is concerned with the detection and prevention of financial fraud and white-collar criminal activities. It is a science of gathering and presenting financial information in a form that will be accepted by a court of law against perpetrators of economic crimes.

2. Defining Forensic Accounting

Forensic accounting definitions commonly refer to fraud, fraud prevention, and fraud investigations as the role of the forensic accountant. While those definitions are not necessarily inaccurate, they provide a definition of forensic accounting only within the specific context of fraud. There are many other contexts beyond fraud to which forensic accounting applies.

Forensic accounting involves the application of special skills such as accounting auditing procedures, finance, quantitative methods, research, and investigations. It also involves knowledge of certain areas of the law. This knowledge combined with these skills enable forensic accountants to collect, analyze, and evaluate evident matter and to interpret and communicate finding.

Key elements of this definition include the following:

Accounting: Forensic accounting is a branch of accounting at its most general level, accounting involves the communication of financial information.

Special skills: Forensic accounting requires special skills that are not required of accountants in general.

Law: Forensic means pertaining to the law. Forensic accounting deals with financial issues that may come before a trier of fact in a court of law or other venue (such as arbitration).

Evident matter: Especially important to forensic accounting is evidential matter that may bear on the truth or falsity of an assertion made before a trier of fact.

Interpretation and communication: In many cases, forensic accountants interpret evidence and communicate expert opinions to clients and a trier of fact.

‘Forensic,’ by definition, means “suitable for a court of law.” It means applying scientific knowledge to the legal issues. Forensic Accounting is a type of accounting that can be used in presentation before a legal forum. Maurice Peloubet, a New York CPA, first coined the term "Forensic Accounting" in 1946 in an essay "Forensic Accounting: Its Place in Today's Economy" , and its inspiration came from the responsibility of reconstructing financial enigmas to prove fraud and embezzlement.

In simple worlds, Forensic Accounting can be described as the act of identifying, settling, sorting, extracting, recording, reporting and verifying financial data in question, as well as clearly organizing and analyzing to make proper conclusions about the state of financial matters that have fallen under criminal observation. It is the application of investigative and analytical skills for the purpose of resolving financial issues in a manner that meets standards required by courts of law. Forensic accountants apply special skills in accounting, auditing, finance, quantitative methods, certain areas of the law, research and investigative skills to collect, analyze and evaluate evidential matter and to interpret and communicate findings

Forensic Accounting and Fraud Examination by Kranacher, Riley, and Wells defines financial forensics similarly, as Financial forensics is the application of financial principles and theories to facts or hypotheses at issue in a legal dispute and consists of two primary functions:

1. Litigation advisory services, which recognizes the role of the financial forensic professional as an expert or consultant
2. Investigative services, which makes use of the financial forensic professional's skills and may or may not lead to courtroom testimony.

Financial forensics is the intersection of financial principles and the law and, therefore, applies the

1. technical skills of accounting, auditing, finance, quantitative methods, and certain areas of the law and research;

2. investigative skills for the collection, analysis, and evaluation of evidentiary matter; and
3. critical thinking to interpret and communicate the results of an investigation.

Crumbley, Heitger, and Stevenson Smith in their book Forensic and Investigative Accounting, Second Edition, provide the definition of forensic accounting: "Forensic accounting is the use of accounting for legal purposes."

They continue in their initial discussions about forensics and accounting to include a much longer but equally understandable definition, as follows:

Forensic accounting is the action of identifying, recording, settling, extracting, sorting, reporting, and verifying past financial data or other accounting activities for settling current or prospective legal disputes or using such past financial data for projecting future financial data to settle legal disputes

In a legal case involving financial fraud or disputes, a special type of expertise is necessary in the investigations that must be carried out to get to the bottom of the situation. The services of a forensic accountant are relied on in such a case. Forensic accounting is the combination of accounting and investigation expertise that are needed to resolve legal disputes involving finances. Thus, accounting skills used with the intent of finding out whether criminal actions have taken place regarding financial matters is termed 'forensic accounting.' Two other terms used to identify a 'forensic accountant' are 'forensic auditor' or 'investigative auditor.'

Forensic accountants need to be familiar with an impressive variety of fields. A forensic accountant must not only understand accounting and investigative techniques, but must also have a working knowledge of economic theories, business practices, financial reporting, data analysis, e-discovery, litigation, and more. A forensic accountant must be able to make sense of complicated financial documents and must be able to readily pick up discrepancies.

In today’s world, large companies may rely on forensic auditors even before they find themselves in a legal battle. Have forensic accountants or auditors look over company books can help prevent legal problems from arising because a financial obligation or liability has not been satisfied.

In an actual case, forensic accountants might examine company receipts to verify reported revenue or examine company financial statements to judge whether or not they provide potential investors with accurate information. Forensic accounting procedures involve the examination of a wide variety of documents, including financial statements, transactions with both clients and investors, tax documents, and more. A forensic accounting report in a court case will be given using court-approved language and structure.

Forensic accountants combine the fields of accounting and law to get to the bottom of financial disputes, and they must understand a variety of different fields involving financial and legal practices. They have become increasingly important in recent years in light of large corporate scandals such as the Enron scandal.

Forensic accounting has become increasingly important in the years since the term was coined with growing complexities in financial markets, the tax code, and the increasing globalization of business. As the field continues to expand, the need for educated professionals is growing too, and for those looking for a more exciting path within an accounting career, forensic accounting is proving to fill that void.

Forensic accounting is typically divided into two areas:

1. Litigation services: The forensic accountant serves as a testifying expert or non-testifying consultant and helps with actual or potential legal or regulatory proceedings before a trier of fact in connection with the resolution of disputes between parties. Litigation services include serving as an expert witness, a litigation consultant (that is, a non-testifying expert), and in various other roles in dispute-resolution or legal processes (for example, as a bankruptcy trustee).
2. Investigative services: The forensic accountant serves as a consultant in cases that do not involve actual or threatened litigation, but do involve performing analyses or investigations that may require the same skills used in litigation services.

3. A Brief History of Forensic Accounting

Forensic Accounting has existed for thousands of years. In ancient Egypt, accountants were known as the eyes and ears of the pharaoh. By some reports, ancient forensic accountants were adept at getting to the truth and, at times, they availed themselves of harsh interrogation techniques and even torture.

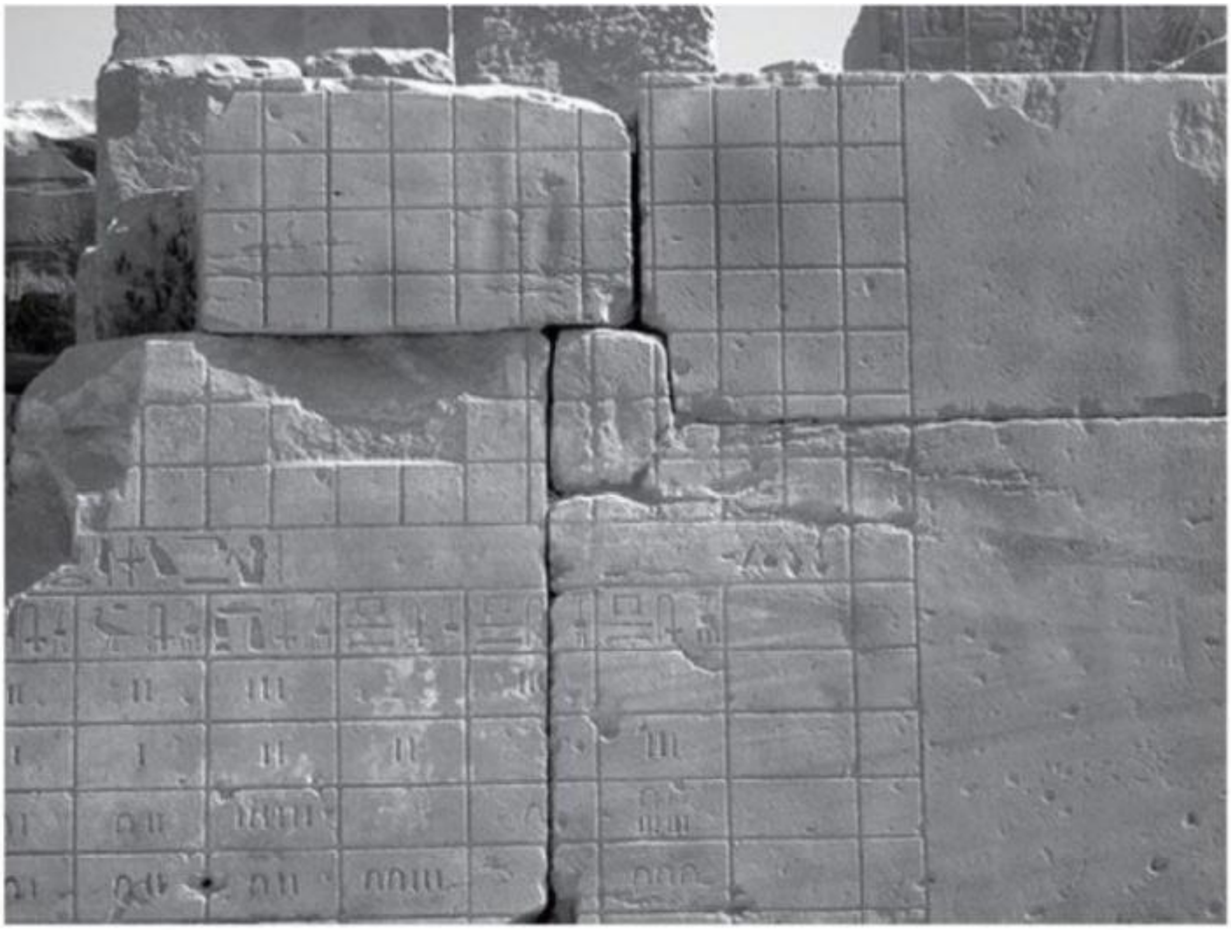

Fig.1 Accounting for offerings at the temple of Karnataka.

In the United States and Canada, perhaps the first case of an accountant testifying in court as an expert witness was in the 1817 Canadian case Meyer V. Sefton. However, it was not until over a hundred years later that the term forensic accounting was coined by Maurice Peloubet in 1946 when he published an article titled, “Forensic Accounting – Its Place in Today's Economy.”

Fig. 2 Maurice Peloubet

Forensic accountants have been around for nearly 200 years. The earliest reference was found in 1824 in an accountant's advertising circular in Glasgow, Scotland. These special accountants gave testimony in court and in arbitration proceedings. Interest in forensic accounting spread through the United States and England early in the twentieth century. One of the first institutions to use the services of such investigative accountants was the IRS. The story of Al Capone the famous mobster being caught on a tax evasion scheme is well-known. The FBI decided to use forensic accountants and employed nearly 500 such agents during World War II. As a profession, forensic accounting continued to grow during the latter half of the century, as GAAP and tax laws became widespread and mandatory.

The following are a few major milestones in forensic accounting:

- 1942: Maurice E. Peloubet published "Forensic Accounting: It's place in today's economy."
- 1982: Francis C. Dykman wrote "Forensic Accounting: The Accountant as an Expert Witness."
- 1986: The AICPA issued Practice Aid # 7, outlining six areas of litigation services – damages, antitrust analysis, accounting, valuation, general consulting and analyses.
- 1988: Association of Certified Fraud Examiners established
- 1988: A new genre of detective novels where the forensic accountant was the star.
- 1992: The American College of Forensic Examiners was founded.
- 1997: The American Board of Forensic Accountants was founded
- 2000: The Journal of Forensic Accounting, Auditing, Fraud and Taxation was founded.

Forensic accounting is hardly a new field, but in recent years, banks, insurance companies and even police agencies have increased the use of these experts. A study conducted by Kessler International (a forensic accounting and investigative firm) showed that there is a growing need for experienced forensic accountants. Todd Avery, president of the risk consulting firm, Kroll Worldwide, says that many executives are paying greater attention to business controls and fraud prevention today than they were doing a few years ago. US News and World Report recently named "Forensic Accountant" as one of the most secure career tracks over the next few years – the profession made the "Twenty Hot Job Tracks" list. Why is forensic accounting so popular now? According to some experts, this increased interest is because of the struggling stock market and lack of investor confidence which has forced many organizations to take a long, hard look at their financial statements. A sluggish economy with its attendant problems might also be an incentive to commit fraudulent acts, thus requiring the services of an expert. The increase in white collar crime and the difficulties faced by law enforcement agencies in uncovering fraud have also contributed to the growth of the profession. Many accounting firms believe that the market is sufficiently large to support an independent unit devoted strictly to forensic accounting. Whatever the reasoning may be, more and more forensic accountants are being called upon to use their investigative skills to seek out irregularities in their companies' financial statements.

4. Forensic Accounting in Comparison

4.1. Forensic Accounting versus Financial Accounting

Accounting involves recording, classifying, analyzing and reporting financial data and information. The emphasis is on converting raw financial data into information useful for decision makers by using an applicable financial reporting framework. The useful information is typically presented to decision makers in the form of financial statements. In summary, the work product of the traditional accountant is one or more financial statements. Financial accounting is the preparation of financial statements based on Generally Accepted Accounting Principles. It is the process of recording, summarizing and reporting a company's business transactions through financial statements. These statements are: the income statement, the balance sheet, the cash flow statement and the statement of retained earnings. Financial accounting professionals are responsible for the public reporting of a company or organization's financial status. This work involves collecting and maintaining data, detecting trends and forecasting future needs. In addition, financial accountants prepare detailed statements and communicate financial information to company leaders and audiences that do not have an extensive accounting background.

But when it comes to typical work product of forensic accountants tends to be much different from that of traditional accountants. The scope of each forensic accounting project is unique and the work product flows from the scope of the particular project. Such work products often consist of a written or oral report of findings or recommendations or both. When testifying before a trier of fact as an expert witness, forensic accountants ordinarily express their findings as expert opinions. In this use, "opinion" is a term of art in judicial guidelines on evidence and the law, and differs from its use in the accounting literature. It is an art of investigation over accounting records, financial statements, and other related financial records. The result of investigation mostly uses for legal support, and resolving conflict. This job requires technical skills in accounting, investigation and legal. The investigation is cover certain areas include fraud, crime, insurance claims as well as a dispute among shareholders. Here the common procedures are financial statement analysis, computer assistance, supporting document examination, investigation, and interview. In general, Forensic Accountants are required to have knowledge and experience in accounting and investigation skills. These are the most important requirements. Also, to be able to perform its works efficiently and effectiveness, knowledge in those related industries that being investigate also consider to be important. These are what drive forensic accounting to become more attractive and highly paid.

4.2. Forensic Accounting versus Auditing

Auditing is related to financial accounting, but differ in several ways. Auditors usually work with companies to review the reports created by financial accounting offices. Audits are a thorough review of a company's financial records conducted by external auditors to verify that their financial statements are accurate and reliable. Audits are also customarily conducted to assess the effectiveness of internal controls or compliance with regulations. Independent audits are conducted with the goal of providing a reasonable assurance of the accuracy of financial statements. Companies awarded government contracts are subject to government audits to verify the contractor has established a system of internal controls to deter fraud in the workplace. In some audits, the auditor may discover symptoms suggestive of fraud. In those circumstances, the audit intersects with fraud examination using the techniques developed to define the who, what, when, where, and how the fraud took place, but also notice that fraud examination includes prevention and deterrence efforts as well as detection and investigation.

A forensic accounting engagement applies accounting, auditing, and investigative skills to examine, analyze, and report on financial information in a manner suitable to the court. An audit is performed by an internal or external auditor, who must adhere to a certain set of standards Forensic accounting is the specialty practice area of accounting that investigates whether firms engage in financial reporting misconduct. Forensic accountants apply a range of skills and methods to determine whether there has been financial reporting misconduct. Speaking simply, virtually all audit engagements have a single objective of expressing one opinion on a set of financial statements whereas each forensic accounting project is very uniquely focused on a client's particular needs and the objective is usually to report recommendations or findings.

Forensic accountants sometimes engage in auditing work, but for purposes other than providing an opinion on an entity's financial statements. For example, a forensic accountant may conduct a forensic engagement as part of an occupational fraud investigation. The result of such an investigation will likely be a report that identifies, for example, the amount of the fraud loss and any control weaknesses that led to the fraud. These fraud engagements are performed as consulting engagements.

Forensic accountants apply specialized skills (in the form of specialized procedures) that differ from those used by auditors of historical financial statements. For example, auditors may use observation techniques whereas forensic accountants may use surveillance techniques. Unlike traditional auditors, not all forensic accountants are required to be independent of their clients in the way the term is used in other accounting literature.

Independence is required, though, when forensic accountants participate in attest engagements such as audits of financial statements for the purpose of opining on the fairness of their presentation and reviews of financial statements.

4.3. Forensic Accounting versus Fraud Examination

Both fraud examiners and forensic accountants work in highly specialized accounting fields requiring additional training and professional certifications. They are involved in investigating financial information in an effort to identify fraudulent activity, but each career has its own specific roles and responsibilities. Fraud examiners can work in any number of industries including government, banking, insurance or information technology. Forensic accountants conduct investigations to support pending or ongoing litigation and may often be called upon to act as expert witnesses in court cases.

Both forensic accounting and fraud examination are different but related. Forensic accounting work is done by accountants in anticipation of litigation and can include fraud, valuation, bankruptcy and a host of other professional services. Fraud Examination can be concluded by either accountants or non-accountants and refer only to anti-fraud.

4.4. Forensic Accounting and the Accounting Profession

The accounting scandals involving Enron, WorldCom, Global Crossing, and other companies have put accountants in the public Spotlight as never before in their history. After these accounting scandals, public confidence in the accounting profession has been seriously undermined. However, the scandals have created business for forensic accountants and developed opportunities for forensic and investigative accounting.

Forensic accountants have been conducting these activities for quite some time in a quiet professional manner. New laws and regulations resulting from these scandals will make the role of forensic accountants more independent than ever before in the business world.

Forensic accountants, also referred to as Forensic auditors or investigative auditors, often have to give expert evidence at the eventual trial. All of the larger accounting firms as well as many medium-sized and boutique firms have specialist forensic accounting departments. Within these groups, there may be some further sub-specializations: some forensic accountants may, for example, just specialize in insurance claims or personal injury claims, fraud construction, Or royally audits.

Forensic accountants utilize an understanding of business information and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and investigative techniques, and litigation processes and procedures to perform their work. Forensic accountants are also increasingly playing more proactive risk reduction roles by designing and performing extended procedures as part of statutory audit, acting as advisers to audit committees, fraud deterrence engagements, and assisting in investment analyst research.

The skeptical mindset is something that has long been inherent in forensic accountants and other internal investigators when looking for evidence of fraud. The investigator historically has asked a set of questions different from those of conventional auditor, who is monitoring the financial statements to see whether they are in compliance with generally accepted accounting principles (GAAP) and thereby fairly represent the financial conditions of the company.

Historically, analysts believed that audited financial statements contained all the information needed for their analysis. This misconception was not only common to companies looking at acquisition targets but was also to be found at banks, bonding companies, vendors' customers, and any other type of business wishing to have some type of fiduciary relationship with another company. The exposed misrepresentations on the financial statements of Enron, WorldCom, and others should sufficiently demonstrate that making an investment decision based solely on financial statement analysis can be dangerous. Financial statement fraud has always been with us, but the recent scandals show that not even the most important companies in the economy can remain untainted. In 1998, then–SEC chairman Arthur Levitt warned in a speech called "The 'Numbers Game'" that aggressive accountants were exploiting the flexibility of generally accepted accounting principles to create misleading earnings reports: "As a result, I fear that we are witnessing an erosion in the quality of earnings, and therefore, the quality of financial reporting. Managing may be giving way to manipulation; integrity may be losing out to illusion."

Fraud auditing, forensic accounting, and/or fraud investigation (i.e., forensic accounting) put things together rather than take them apart, as is the case in financial classical auditing or modern method of systems analysis. The process of forensic accounting is also sometimes more intuitive than deductive, although both intuition and deduction play important parts. Financial auditing is more procedural in many regards and is not intended to work as effectively as the tenets of fraud auditing and forensic accounting.

5. Forensic Accounting Knowledge and Skills

Forensic accounting requires knowledge and skills in many different areas. These areas are overlap each other.

Accounting:

Forensic accounting spans many areas of accounting, therefore broad accounting knowledge and skills are required. However, certain accounting knowledge and skills are required within specialized areas of forensic accounting. For example, a forensic accountant specializing in investigating occupational fraud might not need to be an up-to-date expert in international accounting standards, but would likely need specialized knowledge and skills relating to accounting information systems, digital forensics, and accounting information systems auditing procedures. Similarly, a forensic accountant specializing in estimating economic damages may need business valuation skills.

Auditing:

Auditors are specialists in collecting, interpreting. and evaluating data and information. Such skills are essential to, forensic accounting as previously discussed, when forensic accountants testify before a trier of fact as an expert witness, they ordinarily express their findings as expert opinions. Their findings must be based on evidence, and evidence must be collected and interpreted. Therefore, Forensic accountants should be skilled in collecting interpreting evidence. Finally, as previously mentioned, forensic accounting requires knowledge and skills using specialized gathering procedures.

Investigative:

Special skills and knowledge are required to conduct forensic accounting investigations. These special skills and knowledge include an understanding of how to structure and manage investigations, the types of evidence that may be collected, how to maintain the chain of custody, the legal rights of those under investigation, how to identify different types of fraud schemes, how to conduct interviews, and how to detect deception.

Criminology and Digital Forensics:

For criminal investigations, the forensic accountant should have a basic understanding of the various roles played by crime scene investigators, digital forensics experts, forensic scientists, forensic laboratories, prosecutors, and attorneys.

Almost all crimes these days involve digital devices, including computers Therefore it is helpful for the forensic accountant investigating fraud to have a basic understanding of digital forensics in both the areas of computer forensics and network forensics.

Accounting Information Systems:

Key elements of accounting information systems include internal control and business processes. Internal fraud schemes typically involve the violation of weak or nonexistent internal controls within specific business processes. Therefore, the forensic accountant must have a good understanding, of internal control processes and how they interface with business processes and the accounting information system. For example, a sales-skimming fraud scheme may involve the absence of reconciliation controls in the revenue cycle.

Risk Analysis:

Fraud risk management is an issue commonly dealt with by forensic accountants, Fraud risk management activities include fraud prevention, detection, and response. This type of management begins with fraud risk assessment.

Communication:

Communication skills are essential in all areas of accounting. However, such skills can become even more critical in the area of forensic accounting. Forensic accountants serving as testifying experts often write expert reports that are likely to be subject to intense scrutiny in depositions and cross-examinations at trial. Furthermore, forensic accountants may need to explain their opinions on direct examination at trial, which requires effective presentation skills

Psychology:

Understanding the suspect and, in particular, his or her motivations can aid forensic accountants who perform investigations. Motivation can, for instance, help identify the areas that should be investigated. For example, a CEO may be motivated to compete successfully with a sibling by attempting to increase the market price of stock by artificially inflating net asset values and income.

The law enforcement community has long known that one of the best ways to solve a fraud case is by obtaining a confession. The process of obtaining a confession in financial fraud cases is a very carefully orchestrated one that begins with collecting documentary evidence, proceeds to interviews with non-suspects, and often terminates with an interview with the prime suspect. The key to success in interviewing involves the ability to assess honesty versus deception. Consequently, forensic accountants, at times, are aided by the employment of techniques rooted in psychology, such as the analysis of body language and eye movements.

Information Technology:

The importance of information technology to forensic accountants is closely related to the importance of digital forensics and accounting information systems Information technology is constantly evolving and is an inescapable aspect of many types of forensic accounting work.

Not only do forensic accountants use the latest in technology in their investigations, they must also be aware of evolving technological advances to maintain up-to-date professional skills.

Problem Solving:

If there is any one skill that stands out among the others, it is problem solving. Forensic accountants constantly deal with puzzles and mysteries that offer opportunities to sharpen their critical-thinking skills. In fraud investigations and litigation and dispute resolution, there is always an opposing side, and in many cases the opposing side is highly intelligent and seeks to deceive and cover up the truth. The opposing side might, for example, be a fraudster in an embezzlement investigation, a spouse hiding assets in a divorce, a debtor hiding assets in a bankruptcy, or a potential corporate acquisition target providing false financial statements in order to inflate its value.

Legal:

By definition, forensic work is affected by the legal system. In performing litigation services, forensic accountants assist in the legal and dispute resolution processes. Therefore, the forensic accountant is familiar with the court system, applicable federal and state rules of procedure, and rules of evidence. The forensic accountant often needs a basic understanding of various types of common-law and financial crimes such as conspiracy, money laundering, and embezzlement.

6. Fraud

Fraud evokes a visceral reaction in us. It is an abuse of our expectation of fair treatment by fellow human beings. Beyond that, it is a blow to our self-image as savvy managers capable of deterring or detecting a fraudulent scheme. Whether we react because of values or because of vanity, nobody likes to be duped. Many elements of modern society are focused on maintaining an environment of fair dealing. Laws are passed; agencies are established to enforce them; police are hired; ethics and morals are taught in schools and learned in businesses; and criminals are punished by the forfeiture of their ill-gotten gains and personal liberty—all with a view to deterring, detecting, and punishing fraud. The profession of auditing grew out of society's need to ensure fair and correct dealings in commerce and government

Generally, all acts of fraud can be distilled into four basic elements:

1. false representation of a material nature
2. Scienter—knowledge that the representation is false, or reckless disregard for the truth
3. Reliance—the person receiving the representation reasonably and justifiably relied on it
4. Damages—financial damages resulting from all of the above.

By way of illustration, consider the classic example of the purchase of a used car. The salesperson is likely to make representations about the quality of the car, its past history, and the quality of parts subject to wear and tear, ranging from the transmission to the paint job. The elements of fraud may or may not arise out of such statements.

First, there is a distinction between hype and falsehood. The salesperson hypes when he claims that the 1977 Chevy Vega "runs like new." However, were he to turn back the odometer, he would be making a false representation.

Second, the false statement must be material. If the odometer reading is accurate, the salesperson's representation that the car runs like new or was only driven infrequently, is, strictly speaking, mere hype: the purchaser need only look at the odometer to form a prudent view of the extent of use and the car's likely road worthiness.

Third, the fraudster must make the material false misrepresentation with scienter, that is, with actual knowledge that the statement is false or with a reckless disregard for the truth. For example, the car may or may not have new tires. But if the salesperson, after making reasonable inquiries, truly believes that the Vega has new tires, there is no knowing misrepresentation. There may be negligence, but there is no fraud.

Fourth, the potential victim must justifiably rely on the false representation. A buyer who wants a blue car may actually believe the salesperson's representation that "it's really blue but looks red in this light." Reliance in that case is, at best, naive and certainly not justified.

Finally, there must be some form of damage. The car must in fact prove to be a lemon when the purchaser drives off in it and realizes that he has been misled. Regardless of context, from Enron to WorldCom to Honest Abe's Used Car Lot, fraud is fraud, and it displays the four simple elements noted above.

Fraud is an activity that takes place in a social setting and has severe consequences for the economy, corporations, and individuals. It is an opportunistic infection that bursts forth when greed meets the possibility of deception. The fraud investigator is like the attending physician looking and listening for the signs and symptoms that reveal an outbreak. The Association of

Certified Fraud Examiners defines occupational fraud as: "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."2 Before dealing with the accounting details and the investigation itself, we introduce some attempts by the courts, law enforcement, and regulatory authorities to define fraud. Since the subject of this book is workplace fraud, we then outline the nature of workplace fraud through a look at the accounting cycle. We complete the tour with a look at the motives of fraudsters and the consequences of their acts. The modern definition of fraud is derived primarily from case and statute law, but many of the ancient elements remain. Those roots can be traced to fraud, a Latin noun carrying a wide range of meanings clustered around the notions of harm, wrongdoing, and deceit. The modern definition derived from case law focuses on the intent of the fraudster(s) to separate the trusting victim from property or a legal right through deception for his or her own benefit. This deception involves any false or misleading words or actions or omissions or concealment of facts that will cause legal injury. Criminal prosecution of fraud must prove beyond a reasonable doubt that an act meeting the relevant legal definition of fraud has been committed by the accused. In civil cases, liability must be demonstrated on a balance of probabilities. White-collar crime should be viewed as a subclass of fraud. Fraud includes confidence schemes, art forgery, falsified scientific research data, lying on a resume, and so on. White-collar crime, however, is committed by individuals embezzling, manipulating accounts, taking bribes, and so on at their place of business.

Types of Fraud

No forensic investigation can be undertaken without some knowledge of accounting principles. Accounting is a method of tracking business activities in a particular time period (whether it be a week, a month, or a year). Such tracking is needed internally for owners and decision makers to have timely information on the performance of their business. Although most savvy business owners may have day-to-day control over their business, as companies grow larger and their business becomes more complex, the need for more detailed information increases. However, as recent events have shown, people on the outside of a business also need financial information. Their need for information results from the relationship they have with the particular company. An investor will want to know about results and the company's financial stability. Similarly, a creditor will want to know if his debt is likely to be paid, and a potential investor or vendor will need information on the company before moving forward in a financial relationship.

The accounting system comprises the methods by which companies record transactions and financial activities. It tracks the business activity of an entity and is usually categorized as recording data (i.e., the initial entry into the company's records), classifying information into related items, and then summarizing the data for the end user to readily understand.

Although internal fraud has historically centered on manipulation of accounting entries, recent events have been focused more directly on financial statements and the manipulation of the underlying data. From an early age, accountants are taught that the financial statements are a "snapshot," one point in time to capture the profitability (or unprofitability) and financial position of an entity. The balance sheet should convey the financial position of the business at one point in time (e.g., at the company's year-end), listing the company's assets and liabilities, together with the company's equity.

To understand how fraud occurs within businesses is to understand how the cycles work within an accounting system. Specifically, the cycles are defined as:

1. Sales and Accounts Receivable
2. Payments/Expenses and Accounts Payable
3. Human Resources and Payroll
4. Inventory and Storage/Warehousing
5. Capital Expenditures

Sales and Accounts Receivable

The fundamental concept of any business involves getting business from customers, billing for those goods or services, and then making sure the accounts receivable are collected. In terms of the accounting equation and accounting cycle, the revenues from sales appear on a company's income statement, and the respective accounts receivable appear on the balance sheet. Cash sales would directly affect the cash balance, which is also a balance sheet item.

Within this part of the cycle are steps that a business must undertake to minimize its financial risk. These steps include approval potential for credit before entering into a business relationship; having a system for receiving orders from the customers and then invoicing them; and then collecting the amounts owed from the customers, along with the appropriate system for making adjustments to the account for returns, write-offs, and so on.

Fundamental within this accounting cycle are the safeguards put in place by a company—the internal controls to minimize the opportunity for theft or misappropriation. While no different than other aspects of the accounting cycle, it is relevant to note them here. At the same time, the concept behind these controls is similar for all cycles. Specifically:

Separation of duties. This is a fundamental concept of accounting and one through which companies can prevent a lot of frauds by properly segregating the functions of custody, authorization, and recordkeeping. For the sales and accounts receivable cycle, this would apply to separating the credit function and sales function (thereby minimizing the chances of granting credit to an unsuitable potential customer in order to force a sale). Similarly, sales recording and receipt of cash should also be separated.

Physical safeguards of assets. On the most basic level, this should involve restriction of access to computers by specific password, physical locks, and the use of, for example, lock boxes for customers to mail checks, instead of check and cash handling by company employees.

Audit trail (i.e., adequate and proper documentation of transactions). As with other cycles, the need for adequate documentation in an accounting system is fundamental. At a minimum, this should include prenumbered documents for sales orders, shipping documents, sales invoices, credit memos, and remittance advices (or a computer system that assigns numbers as printed, but with sufficient controls over access limited by specific passwords for users).

Approval process. This process extends to credit approval, write-off approval, and the shipment of products.

Independent checks on the system (whether by an internal audit function or an outside source). While many companies have an internal audit function, others do not consider themselves large enough for such a system. In both cases, the organization needs to have adequate awareness that there is some kind of independent monitoring. This should, at a minimum, include independent preparation of bank and other account reconciliations, supervision, and perhaps the use of an outside accountant as an additional monitor.

This is the most cash-intensive of the five cycles. The most common frauds in this cycle are:

Outright Cash Thefts Cash thefts are the easiest and most common type of fraud to perpetrate in this cycle and are usually carried out through unrecorded sales, under ringing of sales, lapping schemes, and overbilling, among others.

Theft of Other Assets Assets can be stolen by ordering and shipping goods to an address other than that of the business.

Kickbacks to Customers In customer kickback schemes, the fraudster underbills the customer for merchandise and they split the difference or receivables are written off as collectible for a fee.

Front-End Frauds Front-end frauds are committed by the fraudster directing customers to take their business elsewhere or misappropriating a rebate.

Case Study: Accounts Receivable Fraud The bookkeeper of a small but growing bread company prepared bills to be sent to customers and was responsible for collecting payments. Sales were growing through the acquisition of new customers and increasing sales to existing ones. A surprise internal audit revealed, however, that bank deposits were not as large as would have been expected considering the rate of sales growth. An examination of customer copies of sales invoices revealed that the amounts being billed were higher than the amounts being recorded in the cash receipts journal (see below for a discussion of journals) for the same transaction. Office copies of the invoices had been altered to reflect the falsified journal entry. The bookkeeper had stolen more than Rs 15,000 over a period of a year before the fraud was discovered. The bookkeeper was dismissed and agreed to repay the money in order to avoid having the matter brought to the attention of the police.

Payments and Accounts Payable In order to manufacture and/or supply goods and services, a business must obviously procure and pay for the goods and services that underlie their sales.

In terms of the accounting equation and accounting cycle, the expenses appear on a company's income statement, and the respective accounts payable appear on the balance sheet. Similar to cash sales, cash purchases would directly affect the cash balance, which is also a balance sheet item.

As previously discussed for the Sales and Accounts Receivable cycle, the steps and controls for safeguarding a company's assets are of a similar ilk. These steps include approving vendors and ensuring they actually exist and are legitimate businesses; proper processing of purchase orders; proper handling in the receipt and recording of goods and services; recording of liabilities; and processing of cash for payment.

This is one of the accounting cycles that is susceptible to breakdowns in controls, for it involves the flow of funds out from an entity. The safeguarding of a company's assets thus proves just as important, if no more so, in this cycle.

In terms of the accounts that companies typically have in their "chart of accounts" (i.e., their roadmap through their financial statements), this cycle can affect many different balance sheet and income statement accounts. Specifically, the payments and accounts payable cycle can affect balance sheet accounts, including cash, inventory, prepaid expenses, accounts payable (collectively "current assets"), equipment, land and buildings, depreciation ("fixed assets"), and other, perhaps longer-term assets and liabilities.

Similarly, in the income statement, just about every account is affected by this cycle, from cost of goods sold (which typically when deducted from sales results in a company's gross profit) to all of the entity's expenses, such as administration, travel, advertising, professional fees, and taxes, among many others.

Within the same guidelines as for the Sales and Accounts Receivable cycle, fundamental controls are essential, especially over the reconciliation of accounts, including the entity's bank accounts. Without a regular (usually monthly) independent reconciliation of the company's bank accounts, the true financial position cannot be known. Similarly, the propriety of transactions and completeness of information cannot be known. At its simplest level, the person who generates checks, the person who signs checks, the person who mails checks, and the person who reconciles the bank account (or accounts) cannot be one and the same. This is a fundamental principle of accounting, which, while it may not exactly date back to Luca Pacioli, still harks back to Pacioli's quote. Once again: "He who does business without knowing all about it, sees his money go like flies."

Along with the reconciliation process, the concepts of budgeting and tendering and vendor knowledge are also key. These processes also include the segregation of duties, proper approvals, and audit trail through proper documentation. Similar to the other accounting cycles, proper documentation includes prenumbered purchase requisitions, purchase orders, receiving reports, and checks. With the advent of sophisticated computer software, many systems now print this information as documents are generated. This therefore puts the onus on a business to safeguard entry to the accounting system and be in a position to identify who enters the system and when. Limiting access at key points therefore makes it more difficult for one person to compromise the system without collusion.

At the entry level of this cycle, acceptance of a vendor, system controls must include background checks on the vendor in order to ensure that the business exists and is legitimate. Adherence to credit limits is another fundamental control in the safeguarding of the company's assets. Companies should also have bid and procurement policies to ensure competitive bidding and to minimize the opportunity for purchasing managers to compromise their position.

This cycle includes non-capital procurements and payments for goods, equipment, and services used in company operations. The buyer may act alone by setting up shell companies to receive goods misdirected from his company by false invoices. These schemes are often extremely complex and involve bank accounts, mail drops, and even corporate filings for the dummy entities. Procurement fraud is frequently a collusive employee–vendor fraud. The vendor will typically provide a bribe or kickback in return for business or, in the case of tendered contracts, for the employee to rig the bidding in favor of the fraudulent vendor. In another scheme, which may or may not be related to the original procurement scheme, once the vendor has been awarded the contract, the cost of the bribe may be recovered and profits increased by substituting products inferior to contract specifications, billing for work not done, shipping less than ordered, padding overhead expenses, and so on. Collusive fraud is the most common form of acquisition-and-payment fraud.

Case Study: Accounts Payable Fraud

The administrator of the school board in a small city had ultimate authority for all items payable from the board's annual budget. As an administrator, he traveled frequently to education conventions and meetings of administrators in the state capitol and across the country. Although he was an excellent CPA and the day-to-day affairs of the board ran smoothly, his prickly personality did not endear him to the board and made his attempts to get approval for his proposals difficult. Frustrated and increasingly embittered, he saw a way to get back at the board by using his signing authority to approve personal expenditures and write checks to himself. He submitted mileage expenses while using a car leased for him by the board, and he used the board credit card to put gas in his own car. Other bills submitted and approved by himself were for meals and entertainment on weekends and repairs to his car. After his secretary blew the whistle on him, forensic investigators found that invoices for many transactions did not exist. The administrator was dismissed from his job, but no charges were ever laid.

Human Resources and Payroll

By definition, this aspect of the cycle includes recruitment, disengagement, and remuneration of employees and the related underlying data of time records, expense reports, and other related matters.

From an accounting cycle perspective, there are many accounts affected by this function, specifically, cash and taxes payable on the balance sheet and salaries/payroll, tax, travel and entertainment, and others in the income statement.

The safeguards for this cycle are necessary for the prevention of nonexistent (also known as "ghost") employees, falsified hours and overtime, false expense reports, and false medical claims.

Again, the underlying fundamental concepts are similar to those for all other accounting cycles, with the need for proper documentation (i.e., timecards, time sheets, timely entry into a computerized timekeeping system, etc.); proper approval (related to hiring, firing, overtime, travel, etc.), and separation of duties. In terms of the last-named, this would include separating the functions of processing and distributing paychecks and approval and payment of expenses, among others.

This cycle deals with hiring and termination, salaries, timekeeping, expense account reimbursements, and health and other types of employee insurance coverage. Common forms of fraud in this cycle are paying ghost employees, overstating hours worked, overstating expenses, and filing false medical claims. Employee and management fraud can overlap in this cycle, especially in the area of false expense account reports. An important but often overlooked area of personnel fraud is the improper vetting of job applicants. Collusion between a personnel department employee and a fraudster applicant could install a fraudster within the company with untold consequences.

Case Study: Payroll Fraud

A suburban construction company employed several hundred laborers at any given time. With a lean operation, the home office included a one-person accounting department, with a long-serving bookkeeper/controller who coordinated the weekly payroll, printed the payroll checks, placed the owner's mechanical signature on the checks, hand-delivered the checks to the job sites, and reconciled the company's bank account.

It came as no surprise then that, after several years, it was discovered that the bookkeeper had perpetrated a scheme whereby at any point in time, she kept several laborers on the payroll after they had left the company ("ghost employees"). She would endorse the back of their checks and deposit them in her own bank account. At the same time, she paid the withholding taxes, union dues, and other deductions! It was only an alert bank teller who eventually noticed the scheme, after several years and over Rs 600,000 had been taken. The company received Rs 500,000 from its fidelity bond carrier, got back much of the tax and union dues, and reached a settlement with the bank for its lack of oversight.

Inventory and Storage/Warehousing

This part of the cycle encompasses the purchasing function as it relates to the company's inventory, but it also includes the warehousing of product for both manufacture and then resale. Physical control is therefore as important as the other system controls within the other accounting cycles.

The processes for this cycle, from an accounting standpoint, include processing requisitions for purchases, receipt of raw materials and finished goods, storage of raw materials and finished goods, and shipment of goods, among others.

From an accounting cycle perspective, this function affects the inventories on the balance sheet and cost of goods sold in the income statement. Important in this process is the maintenance of an audit trail—specifically, receiving reports, perpetual inventory records, control over requisitions, shipping documents, among others.

As well as the audit trail, proper segregation of duties is also essential to this accounting cycle—for example, separation of warehouse custody and purchase authorization. In addition, those with custody over the warehouse should not conduct, or be the lead in conducting, the physical count of inventory. It also goes without saying that physical security is critical for this particular cycle.

This cycle controls the purchase and storage of goods for later processing and sale or just for sale. The most common frauds in this cycle are ordering unneeded inventory and then stealing it for personal use; committing outright theft; and charging embezzlement occurring elsewhere in the company to inventory losses. These schemes can often become extremely complex and involve loading-dock workers, inventory accounting personnel, truck drivers, and receivers of stolen goods in other parts of the state or country.

Case Study: Inventory Fraud

Auditors doing their annual review of the books of a gold refiner were unable to reconcile the inventory value of the gold carried on the company’s balance sheet with the assessed value. In an attempt to show he was trying to solve the problem, the vice president of finance hired forensic investigators to review the inventory. The discovery of a brass bar of exactly the same weight as a gold bar on the inventory list raised a question in the minds of the investigators. An interview with a smelter worker revealed that brass scrap had been melted down, cast into bars, and added to the inventory. There was no record of brass bars on the inventory lists. Forty-five brass bars had been valued at $8 million on the balance sheet. Another $5 million was classified as gold bars “in transit.” The fraud had been going on for about five years when discovered. It had not been perpetrated for the direct personal gain of the VP of finance and his colluding CEO, but as an attempt to hide the operating losses that would have precipitated a fall in the company’s stock if made public in the annual report. The VP of finance and CEO were both charged with fraud, convicted, and served terms in prison.

Capital Expenditures

This part of the accounting cycle is also known as the capital acquisition and repayment cycle or the financing cycle. It includes the borrowing of funds, the debt of a company, and so on. Several transactions surround this part of the cycle, specifically, recording of debt and interest, payment of interest and dividends, and equity financing, among others.

From an accounting cycle perspective, this function affects cash, liabilities (such as mortgages), capital and retained earnings on the balance sheet, and interest paid and received, among other items on the income statement.

An audit trail will once again assist in the safeguarding of the company’s assets through, for example, control over bank deposits and authorizations for loans. An entity must ensure proper documentation of loans, journal entries, stock certificates, and the like. In addition, duties should be segregated, such as stock issuance and handling of cash, as well as separating accounting from handling of cash.

This cycle accounts for debt and equity financing, interest, and dividend payments. The results of these transactions are reflected on the financial statements of the company. Because these accounts are developed at the executive level, this type of fraud is committed almost exclusively by management. The usual frauds are borrowing company money for personal use, misuse of interest income, and misuse of proceeds from financing.

Case Study: Capital Expenditures

A government agency responsible for overseeing mortgage brokers was concerned that many brokers were borrowing and lending money as if they were licensed as banks or trust companies. The agency made a random selection of brokers and hired forensic investigators to examine their books.

Under government regulations, the brokers' activities were limited to finding specific mortgages and investors to invest in them. In a typical case, an investor would give the broker Rs 50,000 to be put out in a particular mortgage at the prevailing rate per annum to be paid monthly. The investigators soon discovered that one broker had exceeded his authority by issuing so-called corporate notes secured by the company's guarantee rather than by a mortgage. The money was being used instead to purchase property for the broker, who then reduced his risk by selling partial interests to family members or other relatives. By the time the investigators arrived, more than $5 million had been taken in through the issuance of corporate notes and pooled instead of being directed to specific mortgages.

What should have been securely backed mortgages on the balance sheet turned out to be high-risk investments in other ventures that were not paying the rates of return required to service the corporate notes. The broker was meeting his monthly obligations to his investors through borrowings on a bank line of credit and was rapidly getting overextended. In the end, the government agency revoked the broker's license and closed his operations with the help of several banks that took over the mortgages to protect the investors.

Other Types of Financial Fraud

Some frauds that affect business often occur outside the typical accounting cycle. Customer fraud, for example, can severely affect insurance companies through filing of false applications and fraudulent claims, especially those for personal injury. Banks and other financial institutions suffer customer fraud through submission of false financial information on loan applications.

Management fraud deserves special mention in these days of corporate scandals. In addition to theft through the capital acquisition and repayment cycle, management can commit fraud through the manipulation of earnings reported on the financial statements prepared for shareholders and creditors. This type of fraud can affect the stock price, management bonuses, and the availability and terms of debt financing. Enron, WorldCom, Global Crossing, and many others are particularly egregious examples of management manipulation of the financial statements that enriched a few but caused the collapse of company pension plans, enormous losses to innocent shareholders, and unemployment for thousands of staff. These frauds have also contributed to the downfall of a major accounting firm (Arthur Andersen), a spate of suits against others, and the decline in the public's confidence in the accounting profession. As we discuss later in this book, fraudsters often rationalize their deeds by claiming "I wasn't hurting anyone"—clearly, this is far from reality.

Categories of Occupational Fraud

The ACFE divides occupational fraud into three broad categories:

1. Corruption
2. Asset misappropriation
3. Financial Statement Fraud

These are further divided into subcategories shown in the chart below:

Fig. 3 The Fraud Tree

Cash thefts

Cash theft usually occur in three different ways:

1. Fraudulent disbursements
2. Skimming
3. Cash larceny

FRAUDULENT DISBURSEMENTS Fraudulent disbursements use some device such as false invoices or timecards to create a false payment obligation for a company. It is the most common type of cash fraud

SKIMMING Skimming is the theft of cash during its collection but before it is recorded on the company books.

CASH LARCENY Cash larceny is the theft of cash after it has been recorded.

Until recent years, and the full realizable impact of WorldCom, et al., through the loss of jobs and life savings, and the impact on at least one major accounting firm and countless others, fraud was often perceived as a victimless crime. Governments and businesses were seen as so wealthy that the money taken by fraud wouldn't be missed. "They can afford it," is the classic rationalization heard in confessions. Fraud is also viewed as an easy way to get money without running the risk of severe punishment. Dismissal is certainly a possibility, but many employers will, in fact, try to hush up news that they have been defrauded for fear of adverse publicity with their customers, vendors, bankers, and insurers.

6.DETERRENCE, AUDITING, AND INVESTIGATION

The increased size and impact of financial reporting scandals and the related loss of billions of dollars of shareholder value have rightly focused both public and regulatory attention on all aspects of financial reporting fraud and corporate governance. Some of the issues upsetting investors and regulators—for example, executive pay that could be considered by some to be excessive—are in the nature of questionable judgments, but do not necessarily constitute fraud. On the other end of the spectrum, there have been more than a few examples of willful deception directed toward the investing community via fabricated financial statements, and many of these actions are gradually being identified and punished. The investing public may not always make a fine distinction between the outrageous and the fraudulent—between bad judgment and wrongdoing. However, for professionals charged with the deterrence, discovery, investigation, and remediation of these situations, a systematic and rigorous approach is essential.

Without an effective regimen, fraud is much more likely to occur. Yet even with a fraud deterrence regimen effectively in place, there remains a chance that fraud will occur. Absolute fraud prevention is a laudable but unobtainable goal. No one can create an absolutely insurmountable barrier against fraud, but many sensible precautionary steps can and should be taken by organizations to deter fraudsters and would-be fraudsters. While fraud cannot be completely prevented, it can and should be deterred.

THE FRAUD DETERRENCE CYCLE

Deterrence Cycle occurs over time, and it is an interactive process. Broadly speaking, it has four main elements:

1. Establishment of corporate governance
2. Implementation of transaction-level control processes, often referred to as the system of internal accounting controls
3. Retrospective examination of governance and control processes through audit examinations
4. Investigation and remediation of suspected or alleged problems

Fig. 4 Fraud Deterrence Cycle

CORPORATE GOVERNANCE

An appropriate system of governance should be born with the company itself, and grow in complexity and reach as the company grows. It should predate any possible opportunity for fraud. Corporate governance is about setting and monitoring objectives, tone, policies, risk appetite, accountability, and performance. Embodied in this definition it is also a set of attitudes, policies, procedures, delegations of authority, and controls that communicate to all constituencies, including senior management, that fraud will not be tolerated. It further communicates that compliance with laws, ethical business practices, accounting principles, and corporate policies is expected, and that any attempted or actual fraud is expected to be disclosed by those who know or suspect that fraud has occurred. There is substantial legal guidance concerning standards for corporate governance, but generally, the substance and also the vigorous communication of governance policies and controls need to make clear that fraud will be detected and punished. While prevention would be a desirable outcome for corporate governance programs, complete prevention is impossible. Deterrence, therefore, offers a more realistic view. In short, corporate governance is an entire culture that sets and monitors behavioral expectations intended to deter the fraudster. Today, changes in business are being driven by increased stakeholder demands, heightened public scrutiny, and new performance expectations. Critical issues related to governance reform are surfacing in the marketplace on a daily basis. These issues include:

1. Protecting corporate reputation and brand value
2. Meeting increased demands and expectations of investors, legislators, regulators, customers, employees, analysts, consumers, and other stakeholders
3. Driving value and managing performance expectations for governance, ethics, risk management, and compliance
4. Managing crisis and remediation while defending the organization and its executives and board members against the increased scope of legal enforcement and the rising impact of fines, penalties and business disruption.

In our experience, the key elements of corporate governance are:

1. An independent board composed of a majority of directors who have no material relationship with the company
2. An independent chairperson of the board or an independent lead director
3. An audit committee that actively maintains relationships with internal and external auditors
4. An audit committee that includes at least one member who has financial expertise, with all members being financially literate
5. An audit committee that has the authority to retain its own advisers and launch investigations as it deems necessary
6. Nominating and compensation committees composed of independent directors
7. A compensation committee that understands whether it provides particularly lucrative incentives that may encourage improper financial reporting practices or other behavior that goes near or over the line
8. Board and committee meetings regularly held without management and CEO present
9. Explicit ethical commitment ("walking the talk") and a tone at the top that reflects integrity in all respects
10. Prompt and appropriate investigation of alleged improprieties
11. Internally publicized enforcement of policies on a "no exception" or "zero tolerance" basis
12. The board and/or audit committee's reinforcement of the importance of consistent disciplinary action of individuals found to have committed fraud
13. Timely and balanced disclosure of material events concerning the company

14. A properly administered hotline or other reporting channels, independent of management
15. An internal audit function that reports directly to the audit committee without fear of being "edited" by management (CEO, CFO, controller, et al.)
16. Budgeting and forecasting controls
17. Clear and formal policies and procedures, updated in a timely manner as needed
18. Well-defined financial approval authorities and limits
19. Timely and complete information flow to the board

In order to execute effective governance, boards and management must effectively oversee a number of key business processes, including the following:

1. Strategy and operation planning
2. Risk management
3. Ethics and compliance (tone at the top)
4. Performance measurement and monitoring
5. Mergers, acquisitions, and other transformational transactions
6. Management evaluation, compensation, and succession planning
7. Communication and reporting
8. Governance dynamics

All the preceding elements are critical to a good governance process.

TRANSACTION-LEVEL CONTROLS

Transaction-level controls are next in the cycle. They are accounting and financial controls designed to help ensure that only valid, authorized, and legitimate transactions occur and to safeguard corporate assets from loss due to theft or other fraudulent activity. These procedures are preventive because they may actively block or prevent a fraudulent transaction from occurring. Such systems, however, are not foolproof, and fraudsters frequently take advantage of loopholes, inconsistencies, or vulnerable employees. As well, they may engage in a variety of deceptive practices to defeat or deceive such controls. Anti–money laundering procedures employed by financial institutions are an excellent example of a proactive process designed to deter fraudulent transactions from taking place through a financial institution. Another familiar example is policy relating to the review and approval of documentation in support of disbursements.

Literature on this topic is extensive, but one manual in particular is widely recognized as authoritative: Internal Control: Integrated Framework, prepared by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and published by the AICPA. This manual lays out a comprehensive framework for internal control. The critical elements highlighted in the COSO framework are:

1. The Control Environment. This is the foundation for all other components of internal control, providing discipline and structure, and influencing the control awareness of the organization's personnel. Control environment factors include the integrity, ethical values, and competence of the organization's people; management's philosophy and operating style; management's approach to assigning authority and responsibility; and how personnel are organized and developed.
2. Risk Assessment. Effectively assessing risk requires the identification and analysis of risks relevant to the achievement of the entity's objectives, as a basis for determining how those risks should be managed and controlled. Because

economic, industry, regulatory, and operating conditions continually change, mechanisms are needed to identify and deal with risks on an ongoing basis.

3. Control Activities. Control activities occur throughout an organization at all levels and in all functions, helping to ensure that policies, procedures, and other management directives are carried out. They help, as well, to ensure that necessary actions are taken to address risks that may prevent the achievement of the organization's objectives. Control activities are diverse, but certainly may include approvals, authorizations, verifications, reconciliations, operating performance reviews, security procedures over facilities and personnel, and segregation of duties.
4. Information and Communication. Successfully operating and controlling a business usually requires the preparation and communication of relevant and timely information. This function relies in part on information systems that produce reports containing operational, financial, and compliance related data necessary for informed decision making. Communication should also occur in the broader sense, flowing down, up, and across the organization, so that employees understand their own roles and how they relate to others. Further, there must be robust communication with external parties such as customers, suppliers, regulators, and investors and other stakeholders.
5. Monitoring. COSO recognizes that no system can be both successful and static. It should be monitored and evaluated for improvements and changes made necessary by changing conditions. The scope and frequency of evaluations of the internal control structure depend on risk assessments and the overall perceived

effectiveness of internal controls. However, under the Sarbanes-Oxley requirements, management and the external auditors are each charged with performing an evaluation at least annually.

To serve the needs of a thorough Fraud Deterrence Cycle, several aspects of control processes are of particular importance. Among them are the following:

1. Additions/changes/deletions to master data files of customers, vendors, and employees
2. Disbursement approval processes
3. Write-off approval processes (in accounts such as bad debt, inventory, etc.)
4. Revenue recognition procedures
5. Inventory controls
6. Processes for signing contracts and other agreements
7. Segregation of duties
8. Information systems access and security controls
9. Proper employment screening procedures, including background checks
10. Timely reconciliation of accounts to subsidiary ledgers or underlying records

Cash management controls

1. Safeguarding of intellectual assets such as formulas, product specifications, customer lists, pricing, and so forth
2. Top-level reviews of actual performance versus budgets, forecasts, prior periods, and competitors

RETROSPECTIVE EXAMINATION

The first two elements of the Fraud Deterrence Cycle are the first lines of defense against fraud and are designed to deter fraud from occurring in the first place. Next in the cycle are the retrospective procedures designed to help detect fraud before it becomes large and, therefore, harmful to the organization. Retrospective procedures, such as those performed by auditors and forensic accounting investigators, do not prevent fraud in the same way that front-end transaction controls do, but they form a key link in communicating intolerance for fraud and discovering problems before they grow to a size that could threaten the welfare of the organization. Further, with the benefit of hindsight, the cumulative impact of what may have appeared as innocent individual transactions at the time of execution may prove to be problematic in the aggregate. Although auditing cannot truly “prevent” fraud in the sense of stopping it before it happens, it can be an important part of an overall fraud deterrence regime.

INVESTIGATION AND REMEDIATION

Positioned last in the Fraud Deterrence Cycle is forensic accounting investigation of suspected, alleged, or actual frauds. Entities that suspect or experience a fraud should undertake a series of steps to credibly maintain and support the other elements of the Fraud Deterrence Cycle. Investigative findings often form the basis for both internal actions such as suspension or dismissal and external actions against the guilty parties or restatement of previously issued financial statements. An investigation also should form the basis for remediating control procedures. Investigations should lead to actions commensurate with the size and seriousness of the impropriety or fraud, no matter whether it is found to be a minor infraction of corporate policy or a major scheme to create fraudulent financial statements or misappropriate significant assets. All elements of the cycle are interactive. Policies are constantly reinforced and revised, controls are continually improved, audits are regularly conducted, and investigations are completed and acted upon as necessary. Without the commitment to each element of the Fraud Deterrence Cycle, the overall deterrent effect is substantially diminished.

7. Profile of the Fraudsters

Starting with the assumption that most people are honest. It's a nice way to look at the world, and it summons up childhood memories about learning that honesty is the best policy.

Sad to say, human history and human nature tell a different story, and so do the statistics that examine them. While most societies explicitly abhor violent crime and bodily harm, many societies hold financial fraud, whatever its scale, as a less reprehensible wrongdoing. Charles Ponzi, creator of the Ponzi scheme, was celebrated in some quarters as a folk hero and cheered by many of the people he helped defraud. Financiers and executives, whose frauds can disrupt thousands or tens of thousands of lives, have historically been "punished" with relatively light sentences or serve their time at a low-security federal "tennis camp." Some scholars have called this attitude toward white-collar crime "a perversion of our general societal admiration for intelligence."

During much of the past century, psychologists and sociologists struggled to understand the inner workings of people who commit white-collar crime. Edwin Sutherland's White-Collar Crime, the most influential work in the field, argued in 1939 that an individual's personality has no relevance to a propensity to commit such crimes. Rather, he said, economic crimes originate from the situations and social bonds within an organization, not from the biological and psychological characteristics of the individual. Sutherland also made the useful, if apparent, observation that criminality is not confined to the lower classes and to social misfits but extends, especially where financial fraud is concerned, to upper-class, socially well-adjusted people. Later authors introduced quite different ideas—for example, suggesting that financial fraud is an inevitable feature of capitalism, in which the culture of competition promotes and justifies the pursuit of material self-interest, often at the expense of others and even in violation of the law.

Over the many decades since White Collar Crime was published, persuasive studies have argued that two factors should be considered in analyzing the psychology and personality of the fraudster:

1. The biological qualities of an individual, which vary widely and influence behavior, including social behavior
2. The social qualities that are derived from and in turn shape how the individual deals with other people.

From these studies of psychology, two general types of financial fraudster have been observed:

1. Calculating criminals who want to compete and to assert themselves
2. Situation-dependent criminals who are desperate to save themselves, their families, or their companies from a catastrophe

Since these studies were published, a third type of criminal has emerged out of catastrophic business failures and embarrassments. We will call them power brokers.

CALCULATING CRIMINALS

Calculating criminals are predators. They tend to be repeat offenders, they have higher-than-average intelligence, and they're relatively well educated. They usually begin their careers in crime later in life than other criminals. These predators are generally inclined to risk taking—no surprise there—and they lack feelings of anxiety and empathy. A related view, somewhat different in its emphasis, was offered in a 1993 study of Wall Street's insider-trading scandals by a team of psychologists who suggested that individuals willing to commit such crimes had an "external locus of control"—that is, they lacked inner direction, self-confidence, and selfesteem and were motivated by their desire to fit in and be accepted. Furthermore, the study found that they define success by others' standards.

SITUATION-DEPENDENT CRIMINALS

But the vast majority of corporate criminals are not predators at all. They are situation-dependent criminals: seemingly ordinary people who commit crimes without the intent to harm others. This is a key to understanding white-collar crime, because almost all news coverage and much of the scholarly literature in the area focuses on "egregious, highly publicized, and largely atypical cases" and ignores "the more common, run-of-the-mill, garden-variety" offenders and offenses that account for most white-collar crimes.

This category of financial fraudster—run-of-the-mill, garden-variety, but still capable of doing great harm.

This white-collar criminal profiled below don't stand out. Many employees share these characteristics.

Typical White-Collar Criminal

1. Older (30+ years)
2. 55% male, 45% female
3. An appearance of a stable family situation
4. Above-average (postgraduate) education
5. Less likely to have criminal record
6. Good psychological health
7. Position of trust
8. Detailed knowledge of accounting systems and their weaknesses
9. Prior accounting experience

POWER BROKERS

Many of today's once highly placed corporate criminals show characteristics of each of the previous two categories, but they are different enough in their methods and motives to deserve a category all their own: power brokers. Like many of us, you have read about their excesses and asked yourself how respected business leaders could have been so deluded as to believe that they could usurp the financial and human resources of their companies to line their own pockets and deceive a wide range of stakeholders, including their own employees.

Did the corporate leaders now facing criminal charges begin their careers with the intention of creating a company that would enrich themselves while eventually destroying the dreams and plans of thousands of innocent victims— employees and investors alike? Were all of them predators? Probably not. But a combination of predator characteristics and the circumstances of their positions led them to commit financial crimes.

Despite the deficiencies in gathering evidence and developing theory, several studies have been done that show some consistency. For those of us who write and speak regularly on the subject of financial fraud, in general terms we typically describe the perpetrator as someone who has experience, is placed in a position of trust, and who will have to be in a position of having the opportunity to commit the crime.

Women commit just about as many frauds as men, but the median amount is smaller. Fraud, too, has its "glass ceiling" Most executive and managerial positions are still held by men, and their opportunities to steal large sums are greater. Fraudulent acts by women seem to increase as one descends the occupational hierarchy. The activity of women is especially marked at the clerical levels of the financial industry. One can reasonably expect that the admission of greater numbers of women to positions of power will result in a more equitable balance in the gender statistics.

Frauds by persons with university education are less frequent but involve larger median amounts than those committed by persons with only high school or below. Once again, this reflects the fact that educated people tend to rise to higher levels of responsibility and thus control larger amounts of money.

Perhaps the most disturbing statistic in the ACFE study is the one showing that only 12 percent of fraudsters had previous convictions for a fraud-related offense, which means 88 percent of the frauds were committed by persons who had never been charged with or convicted of any previous crime. This is consistent with Romney et al. and Weisburd et al., who discovered no sociopathic behavior patterns in the fraudsters studied in their research.

What, then, makes a person commit that one act that turns a respectable citizen into a criminal? How does a person who does not have the statistical profile of the common criminal form the intent to break the law? Weisburd and Waring identify two broad classes of offender: crisis responders and opportunity takers.

The crimes of the crisis responders “seem to be situational responses to real stress or crisis in their professional or personal lives.” The crimes of the opportunity takers seem to be “linked strongly to some unusual or special set of opportunities that suddenly materialize for the offender.” The crisis responders were people in positions of trust who saw a criminal act as the way out of a perceived financial crisis. These events were anomalies in their social histories. The women acted to pay family bills, and the men stepped over the line for a variety of reasons, such as financial troubles at the company they owned or to reduce their income taxes payable.

The opportunity takers were not driven to commit a crime by financial pressures; they were drawn in by the temptation created by an unusual opportunity. Many of these events were isolated wrong choices. This group, however, also includes those recruited into conspiracies operating in permissive environments. Once involved, these offenders become socialized into criminal activity that can last for years or even decades. The offense for which they suffered their one arrest was, in fact, often one long, systematic criminal activity.

The commission of a crime requires a place that connects opportunity and victim. The most harm is done by officers and managers colluding with others in ways that exploit an organization for which they work. This is the quintessential middle-class crime. Owners and sole proprietors may be from a higher social class, but the businesses they control are usually too small to permit the magnitude of the thefts possible from large corporations. Others of high social status, such as doctors and lawyers, rarely commit large complex crimes. Exceptions are those doctors who open clinics to exploit Medicaid.

It is the officers and managers who hold their positions in large companies through education and hard work rather than birth who have the opportunities to commit the big frauds. This is because they command the accounting systems as well as the controls that should safeguard those same systems. These crimes are most frequently collusive because their commission requires an assembly of skills capable of exploiting the complexity of the corporate structure.

KINDS OF RATIONALIZATION

In many admission-seeking interviews, suspects confess to their crimes, but rarely do they say, “I stole the money.” Instead, they bring up their rationalization for the crime. Such rationalizations can be of many kinds:

- “It was a loan, and I had every intention of paying it back. See (pulling out a spreadsheet), I kept track of all my loans so that I could pay it all back one day.”
- “That accounting rule is confusing and subjective. Accounting for the transactions in the manner I chose is entirely acceptable.”
- “My boss has been cheating on his taxes for years. I’m just getting my share.”
- “Everyone in this industry takes kickbacks. I’m sure my employer is aware of it, and that’s why they don’t pay me very much. They expect me to supplement my income with ‘gifts’ from our suppliers.”
- “I’m the hardest-working employee here, and I know my boss would give me a substantial raise if he could do it without other people knowing. Instead, I take a little bit, but I’m actually saving the company money because only I get the ‘raise.’”
- “What do you expect me to do? You give me no health insurance coverage, and I need to provide for my children and my parents. They depend on me, and I can’t let them down.”
- “There are a lot of good people here. If I didn’t make up a few entries to give the appearance to corporate that we were making budgeted income, they would close our division and put 50 people out of work. I did it to save their jobs.”

In sum, rationalization enables a person to take that final step toward crime.

8. Detection

In the ACFE's 2004 survey, approximately 40 percent of cases were initially detected by tip, approximately 24 percent by internal audit, 21 percent by accident, 18 percent by internal controls, 11 percent by external audit, and 1 percent notified by police.

Since the victims of white-collar crime rarely know anything has happened at the time the action occurred, often a long lag develops between the commission of a crime and its discovery and report. The ACFE notes that the majority of tips came from employees (almost 60 percent), along with tips from customers (20 percent), vendors (16 percent), and anonymous tips (13 percent).

In the recent PwC study noted earlier, internal audit was disclosed as the most successful of all processes in the management of fraud. Matching this study with the ACFE, which showed internal audit accounting for 24 percent of initial detection, should give us a pretty good clue as to where resources should perhaps be spent in organizations. However, for every point in the world of fraud detection, there is a counterpoint, and many smaller business owners will tell you their organization is too small for an internal audit department and they cannot afford such a luxury. Perhaps this then ties in with the fact that companies with fewer than 100 employees accounted for almost 46 percent of cases in the ACFE study, the largest group in the study. Companies with over 10,000 employees accounted for just over 13 percent, the smallest group in the survey.

In a 2001 article, "The Psychology of Fraud,"18 the authors noted that fraud, "like other crime, can best be explained by three factors: a supply of motivated offenders, the availability of suitable targets and the absence of capable guardians—control systems or someone to mind the store."

Financial motivators obviously have a big impact on the cause of financial crime. These can range from an employee with an inability to pay her domestic bills to a senior executive under financial strain because he knows that market factors have adversely affected the business and analysts will be watching the latest results with eagerness. In this case, the strain may go beyond pure financial impact, but also to stature and reputation.

Some theorists have taken a big-picture approach and argued that white-collar crime is the inevitable outcome of the competitive ethic of capitalism. According to this theory, competition is the field on which egotism and recklessness can have full play. We are constantly bombarded by images of the wealth and success that can be achieved through winning in the great experiment in social Darwinism in which we live. The inevitable result of such competition is the recognition of the economic inequality of winners and losers, which can be internalized as the constant fear of failing. This discontent may be sufficient to make a person see white-collar crime as the great equalizing act. The drive for money and the trappings of success are, therefore, the motivators of the act.

Recent theorizing has shifted the focus to the situation in which the crime is committed. This newer thinking does not dismiss the role of personal history, which is so important in the creation of the street criminal, but questions its explanatory power. It raises the question of why certain people commit certain crimes in certain situations. This is a useful line of theorizing since it allows the criminal act to be conceptually distinguished from the criminal's life story and explained as the pursuit of short-term gratification and not the culmination of a long history of personal disadvantage.

The situation in which the potential white-collar offender finds him- or herself plays a most significant role in determining whether a crime will be committed. The corporate culture lived daily at the workplace can often create enormous pressures to commit criminal acts. Examples are common in the famous cases of price-fixing, bribery, and manufacture of dangerous products that occurred throughout the last century. A corrupt corporate culture can lead to the inversion of all values. The comfort of conformity then becomes the Achilles' heel of the middle-class person under pressure to "go along to get along." Loyalty can easily slip into complicity. Criminal behavior becomes normal. Team-playing becomes conspiracy. Fear of dismissal, ostracism, or losing the favor of superiors can be compelling forces in the world of a department or small company. In such an atmosphere, one learns criminal behavior "in association with those who define such behavior favorably," as Sutherland contended.

These acts cannot be explained by a personal history of instability and deviance since stability and conformity are the principal characteristics of these criminals' lives. Even while committing the crimes, white-collar offenders are able to lead their conventional lives, which are, indeed, their camouflage. Their conventionality and stability are the foundation of the trustworthiness that gives them the opportunity to commit the crime in the first place. It is this life of conventionality that gives the criminal act the character of an aberration.

It is, however, the white-collar criminals' power of rationalization that is one of the most amazing aspects of their behavior. They are able to behave normally and aberrantly at the same time without feeling conflict. This behavior is possible through the use of techniques of "neutralization."24 These are acts of mental deftness that allow persons to violate behavioral norms without simultaneously seeing themselves as deviant or criminal. Such self-exculpating explanations can occur both before and after the commission of a criminal act.

The most common rationalization noted several times already in this chapter is that financial crimes do not hurt other people. Embezzlers commonly tell themselves they are merely “borrowing” the money and intend to return it later without anyone else being affected. Many embezzlers justify it because they had to do it to pay mounting family bills. “Everybody’s doing it” is frequently heard as an argument for systematic wrongful company behavior. Corporate offenders often consider laws as an unjust or unnecessary form of government interference disrupting free market forces. They may even argue that breaking the law was necessary for the survival of the company.

Employees frequently offer a moral justification for their thefts with the argument that their employer “owed” them the money. Fraud simply expressed their grievance. For example, they feel exploited and underpaid or hurt after receiving a smaller-than-expected bonus. Many feel justified after being passed over for promotion; others feel they can do the job just as well as, if not better than, the person with the higher education. Personal antipathies, anger after a reprimand from the boss, and the like can all be self-serving explanations for fraud. Such a sense of being wronged, whether justified or not, can fester for years before developing into a plan to defraud.

In rare cases, mental illness can drive a person to commit fraud through a wish to damage the company. Others can be motivated by pure egotism; they commit fraud just to show how smart they are. Yet others are driven by anticapitalist ideologies and think they are destroying the system from within.

9. NEED FOR UNDERSTANDING THE MIND OF THE FRAUDSTER

In the introduction to Why Smart People Do Dumb Things, Mortimer Feinberg and John J. Tarrant begin:

"If you are of above average intelligence—and if you have mastered the use of high intelligence to solve problems and achieve goals—it is the premise of this book that you are at risk [of perpetrating a fraud] because of the strength of your cognitive equipment."

The book recounts tale after tale of successful professionals and politicians who did something dumb and ruined their lives. It is also a book that can help auditors understand the mind of the white-collar criminal. Because auditors, within the time at their disposal, cannot verify every transaction, they must make assumptions based on audit evidence gathered until the point of the decision. The more auditors understand about why criminals do what they do, the better prepared they may be to determine the nature, timing, and extent of audit procedures relative to the risks identified during the planning stage and modified, as may be warranted, on the basis of the audit evidence found. Professional skepticism is the attitude that must drive the financial statement audit. If we lived in a perfect world in which no one made mistakes, or lied, or cheated, or stole, audits would be unnecessary. But we don't, and so audits are required. Even with effective auditing, at the end of every audit and forensic accounting investigation, uncertainty will remain.

As auditors continue to focus on the fact that smart people do dumb things and on the conditions under which white-collar criminals may act, auditors may be able to better select transactions worthy of expanded testing and know also how to evaluate the results of those tests. The so-called fraud triangle, offers three conditions that tend to be present when frauds occur:

1. Incentive or pressure
2. Opportunity
3. Rationalization and attitude

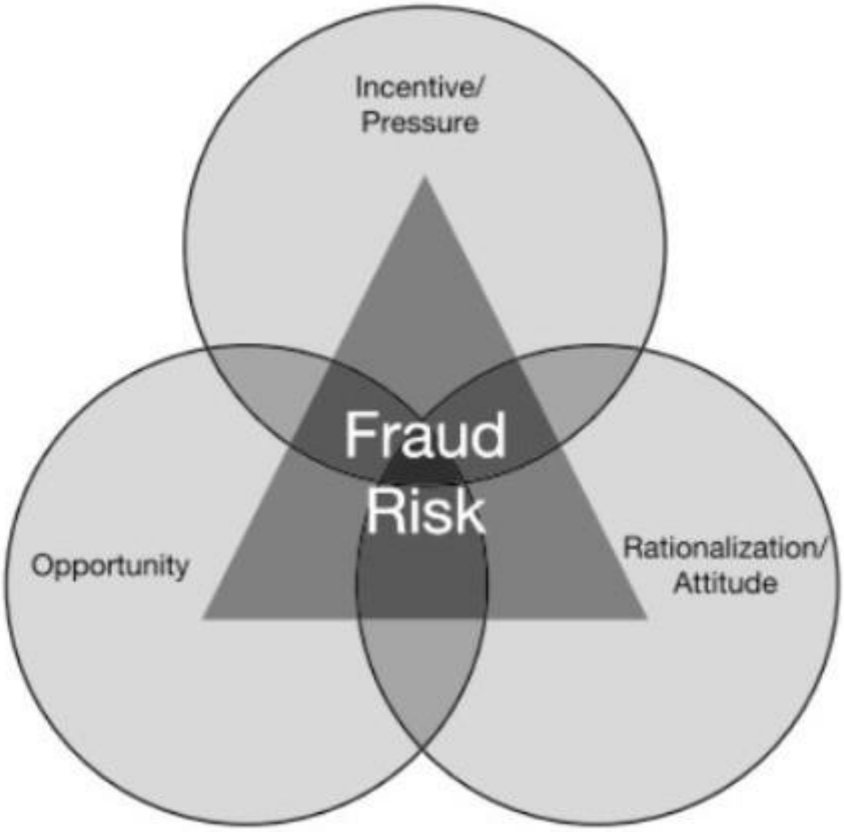

Fig. 5 Fraud Risk triangle

Within each of these broad risk categories, many different and specific potential red flags may be visible within a company.

INCENTIVE AND PRESSURE

Management or other employees may find themselves offered incentives or placed under pressure to commit fraud. When, for example, remuneration or advancement is significantly affected by individual, divisional, or company performance, individuals may have an incentive to manipulate results or to put pressure on others to do so. Pressure may also come from the unrealistic expectations of investors, banks, or other sources of finance.

Certain risk factors are usefully considered in the evaluation of whether or not the organization is at a greater or lesser degree of risk, owing to incentives or pressures that could potentially lead to material misstatements. These risk factors include:

- Circumstances that threaten the profitability or financial stability of the business
- Excessive pressure on management to meet or exceed the expectations of third parties, including investors and lenders
- Significant threats to the personal wealth of management as a result of the performance of the business
- Excessive internal pressures on divisional or departmental management imposed by the board of directors or senior management
- A struggle to retain the company's listing on a stock exchange or debt rating
- Inability to meet debt covenants or satisfy conditions in merger or acquisition agreements
- Incentive and pressure can take a variety of forms within an organization: bonuses or incentive pay representing a large portion of an employee or group's compensation; triggers built into debt covenants tied to share price targets and levels; significant stock option awards throughout the organization but particularly to top management; and aggressive earnings-per-share and revenue targets set by top management and communicated to analysts, investment bankers, and other market participants, with resultant pressure from these groups.

With regard to the risk of material misstatement due to misappropriation of assets, the risk factors are:

- Personal financial problems that might motivate an individual to misappropriate assets
- Adverse relationships between the entity and one or more of its employees, which might create feelings of resentment or disloyalty
- Personal pressures have increased significantly in recent decades as stock options became a common means of compensating and motivating management. Many managers today have a large portion of their compensation and even their net worth tied to the performance of the company and, specifically, the performance of the company's stock. As a result of compensation and retirement contributions in the form of stock grants and as a result of stock ownership and personal debt secured by stock, the financial position of many managers is inextricably tied to the financial performance of their employer. Fear of losing one's position or of delivering bad news, the desire to be promoted, personal financial obligations, or simply greed can also be the driving forces behind fraudulent activity.
- Determining the presence and degree of these pressures or incentives is part of the auditor's goal in evaluating the risk that misstatements due to fraud may have occurred. Keep in mind that some people will go to extraordinary lengths to satisfy their needs. The ability to satisfy those needs through inappropriate measures is increased if the other components of the fraud triangle are present.

OPPORTUNITY

Circumstances may exist that create opportunities for management or other staff to commit fraud. When such opportunities arise, those who might not otherwise be inclined to behave dishonestly may be tempted to do so. Even individuals under pressure and susceptible to incentives to perpetrate a fraud are not a grave threat to an organization unless an opportunity exists for them to act on their need. An opportunity must exist to commit fraud, and the fraudster must believe the fraud can be committed with impunity. Absent or ineffective controls, lack of supervision, or inadequate segregation of duties may provide such opportunities. Opportunities may also be inherent in the nature, size, or structure of the business. Certain types of transactions lend themselves more than others to falsification or manipulation, as do certain kinds of balances or accounts. Certain corporate and group structures may be more opaque and susceptible to misuse. And certain types of asset are more prone to misappropriation.

Risk factors indicative of opportunities that could lead to material misstatements as a result of fraudulent financial reporting include:

- Factors related to the nature of the industry in which the entity operates, the nature of the entity's business and the transactions it enters into, and the manner in which they are recorded in the profit-and-loss account or balance sheet.
- The nature of the entity's relationships with customers and suppliers and its position in its markets: the ability to dominate or dictate terms may create the opportunity for inappropriate or non–arm's-length transactions.
- The degree of judgment involved in determining the level of income or expenditure or the valuation of assets or liabilities: Generally, a higher degree of judgment will give rise to a greater opportunity for deliberate manipulation.

- The extent and effectiveness of supervision of senior management by independent corporate governance functions such as the audit committee, nonexecutive directors, and supervisory boards.
- The degree of complexity and stability of the entity or group.
- The overall control environment, including the continuity and effectiveness of internal audit, information technology, and accounting personnel as well as the effectiveness of accounting and reporting systems.

In several large financial statement fraud cases, opportunity existed by virtue of management's role in the internal control structure and its ability to override or avoid existing controls. With regard to the risk of material misstatement resulting from misappropriation of assets, the risk factors best categorized as related to opportunity can be summarized as follows:

- Susceptibility of fixed assets, inventories, or other assets to misappropriation, depending on such variables as value, demand, portability, and convertibility
- Weaknesses in the controls designed to safeguard assets, such as supervision, segregation of duties, employee screening, physical controls, reconciliations, and other accounting controls

RATIONALIZATION AND ATTITUDE

Some individuals are more prone than others to commit fraud. Other things being equal, the propensity to commit fraud depends on people's ethical values as well as on their personal circumstances. Ethical behavior is motivated both by a person's character and by external factors. External factors may include job insecurity, such as during a downsizing, or a work environment that inspires resentment, such as being passed over for promotion. The external environment also includes the tone at the top—the attitude of management toward fraud risk and management's responses to actual instances of fraud. When fraud has occurred in the past and management has not responded appropriately, others may conclude that the issue is not taken seriously and they can get away with it.

Risk factors that fall into this category of rationalization and attitude are typically the least tangible or measurable, and many are by nature difficult for an auditor to observe or otherwise ascertain. Fundamentally, rationalization and attitude are functions of the culture of an organization, the psychology of those who work in it, and the interaction between the two—for example, the level of employee loyalty to the company. The wider business environment must also be considered: hard times in an industry or in the overall economy may make it easier for some individuals to rationalize fraud. Risk factors to look for, in this somewhat intangible but critically important category, include:

- Lack of clarity or communication about corporate ethical values or infrequent communication and reinforcement of such values
- Disregard for the risk of fraud—or ineffective measures when fraud rises
- Lack of realism in budgeting and forecasting and in communicating expectations to third parties
- Recurring attempts by management to justify inappropriate accounting or disclosure policies and practices on grounds of materiality or other grounds
- Difficult relationships with the entity's auditors: a bullying attitude, imposition of unreasonable time pressure, or constraints on access to relevant audit evidence

Most frauds begin small and build over time. Many people can easily rationalize small infractions such as using the office phone for personal long-distance phone calls or stocking their home office with supplies from the company supply cabinet—and the auditor will come into contact with individuals who are, of course, capable of these rationalizations. These rationalizations can be simple, even for a complex financial crime. Some of the most common rationalizations prove to be the following:

- It is just temporary.
- The company will do better next quarter and the act can be reversed. No one will ever know.
- It is not really fraud, right, if I book this entry one month and then reverse it the next? In the end, it washes and no one's harmed. The company stays in compliance with debt covenants, and we make our dividend payments.
- Management does not care.
- Management does not seriously monitor internal controls.
- Management does not correct known deficiencies in controls.
- Management does not discipline this kind of behavior.
- Management participates in, expects, and rewards this kind of behavior.
- Management has entered into certain transactions purely for the purpose of meeting specific reporting objectives.
- Management traditionally uses aggressive accounting policies, and we need to remain consistent with prior periods.
- The people being promoted helped the company achieve its objectives without regard to the means of getting there.
- Risk taking is rewarded. We are cowboys—but nobody is allowed to say that anymore.
- No one is hurt and the company is helped.

- It is not material to the company as a whole. But it makes a huge difference to our proceeds from the public offering.
- I deserve this.
- I was passed over for the promotion I deserved.
- I'm paid at less than the market rate for my services and the value I provide.
- The company has no loyalty to its employees; I'm likely to be laid off soon.
- This will make up for the benefits the company just eliminated.

Determining whether a basis exists to rationalize a fraudulent act is a key part of the evaluation of the risk that misstatements due to fraud may have occurred. Typically, all three conditions of the fraud triangle will be present in varying degrees when fraud occurs. They are closely related. When the incentive to commit fraud is strong, it is likely to be easier for perpetrators to rationalize their actions. Easy opportunity may have a similar effect: when internal controls are absent or ineffective, an employee may conclude that management is indifferent to fraud—that "nobody cares." The greater the extent to which all three conditions are present, the greater the likelihood that fraud will occur. Cultivating an environment that minimizes these conditions is vital to avoiding or limiting fraud risk. However, even if one or more conditions are absent, fraud risk is not eliminated. The incentive or pressure may be such as to drive an individual or group to commit fraud despite the absence of easy opportunities to do so. Similarly, predators may not need to rationalize their depredations on a firm: it just comes naturally.

It is sufficient to know that it takes all three conditions for a fraud to occur. The first two parts of the triangle, incentive and opportunity, are usually observable. The third condition, rationalization, is usually the toughest of the three to identify. This is why auditors need to be ever vigilant to the possibility of fraud. A more informed understanding of the psychology of the fraudster usually makes for a better auditor.

As auditors focus on the number of people they encounter in the course of an audit, they would probably agree that a great many of those people would no doubt have opportunities to commit fraud. How many others also have the undisclosed incentive and ability to rationalize that are demonstrably part of the fraud triangle? There is no easy way to judge this.

In the design of controls to prevent financial crime and in the performance of audit procedures, it is important to keep in mind the expression, "Locks on doors keep out honest people." Predators, as noted earlier, have a good chance of circumventing most of the controls a company puts in place. Fraud deterrence and detection controls are designed, theoretically, to stop everyone else, but they won't, because it is unrealistic to expect controls that can be designed to stop everyone. Collusion, for example, may well defeat a well-designed control and may not be detected in a timely manner by individuals performing daily control activities. The best fraud deterrence mechanism is simple: create the expectation in your organization that wrongdoers will be caught and that punishment will be swift and commensurate with the offense. The emphasis on expectation is important. It can be brought about in a number of ways. Effective training and education on the importance of ethical conduct, background checks on all employees, regular fraud audits by forensic accounting investigators, and a strong internal control system are among the means. To create that perception, employees must also be well aware that their activities are being monitored, and all employees with access to financial assets and transactions must have a healthy respect for the robustness of the control system. If employees believe they will be caught and punished for wrongdoing, that belief may be enough to keep them from adding rationalization to incentive and opportunity.

Some experts have suggested that attention to the institutional level rather than the individual level can be fruitful. For example, Susan P. Shapiro wrote in American Sociological Review, "I suggest we begin sampling from settings of trust—legislatures, pension funds, hospitals, labor unions, probate or surrogates' courts, charities, law enforcement agencies, wire services, purchasing departments, universities—and examine how these fiduciaries define and enforce trust norms, the structural opportunities for abuse, the patterns of misconduct that ensue, and the social control pressures that respond." This would provide greater understanding, she says, of the conditions that allow the individual to rationalize.

Be that as it may, auditors—working as necessary with forensic accounting investigators—realize that there could be a fraudster somewhere in the organization they're auditing. The fraudster may be a predator—an individual who works there to steal—or may be a seemingly upstanding citizen with a secret incentive such as a problem at home, a "golden" opportunity such as knowledge of a weakness in the control system, and a rationalization such as, "It doesn't really harm anyone." There is another possibility: outright greed.

When fraud is suspected, the first job of the investigative accountant is to discover and review the evidence to prove or disprove the allegations. Since the reputations of the suspected principals are at stake, the evidence-gathering process must be extremely discrete. Evidence must also be gathered and preserved in such a way that it can meet the standards-of-proof tests of any court; this is the forensic standard to which investigative accounting is held. In criminal cases, the evidence must establish guilt beyond a reasonable doubt; in civil cases, liability is established by the less rigorous standard of the balance of probabilities. Nonjudicial regulatory authorities, boards, and tribunals have yet other standards with which the investigator should be familiar.

Evidence will typically come from two primary sources. The first is the accounting records and any underlying documentation that may exist. In many cases, evidence found in these records might suggest additional research in external databases such as public records and court documents, as mentioned above. The investigator's experience should indicate what issues are well supported, which ones need additional evidence, and which are merely circumstantial.

The second source of evidence is gained through the interview process. Interviews may be conducted with key internal personnel, outside sources, and, ultimately, the suspects and any outside parties such as vendors or contractors who have done business with the individuals in question. The nature and timing of the interviews will be driven by the conduct of the case.

The financial investigator must also be a good psychologist and be able to assess the greater or lesser likelihood that any given suspect is a fraudster. The paper and electronic evidence may show that accounting irregularities exist, but unless the evidence is connected to individuals, no fraud can be established. The investigator must be able to pick up on the motivational and behavioral clues that define a suspect. A winter tan, a better car, an affair, domestic financial worries, and a thousand other clues can all raise suspicions that might develop into a picture of criminal activity.

10. Financial Frauds

Ponzi Schemes

In 1919 and 1920, Charles Ponzi operated an investment scheme through his business, Securities Exchange Co., which promised investors returns of up to 50 percent, purportedly to be earned from investing in and arbitraging International Postal Union reply coupons. In reality, after some initial success in his venture, Ponzi sustained losses and to keep the scheme going, began repaying old investors with funds provided by new investors. Although Ponzi was exposed, jailed, and eventually exiled back to Italy, where he died penniless, his name lives on to identify a kind of financial fraud that depends on claims of astonishing profits to investors in the form of rates of return, on attracting more and more new investors to provide the funds repaid to old investors, and on a pyramid structure in which only the initial investors and the sponsor of the scheme recover their investments and earn profits thereon. Modern versions of Ponzi schemes may involve multiple pledging of assets claimed to be security for the investors' loans or other investments, commingling of funds and diversion of cash collateral, and fraud in the inducement to invest by:

- Mischaracterizing the nature of, and risks associated with, the investment
- Overstating anticipated returns and misstating the security backing up the investment
- Misstating financial statements by overstating investment returns and operating results and/or understating losses
- Misrepresenting the success of the product, service, or financial scheme upon which the investment is to be based

- Concealing losses and the failure of the scheme—at least for a time—by paying out later investors' monies to earlier investors

Bank Frauds

Although they are not usually investors in equity securities, banks invest in loans to entities that are based at least in part on reliance upon the financial statements and other financial information provided by the borrower. Thus, fraudulent financial statements may be used to defraud lenders just as they defraud equity investors: usually by overstating a company's financial condition and results of operations. Several additional forms of fraud may also affect lenders. Typically, they involve overstating the value of collateral, pledging fictitious collateral, multiple pledging of assets as security, and fraudulently conveying assets— against which loans were made—to related parties, third parties, or other lending institutions.

In the special case of so-called floor-plan loans, a fraud can be committed by manipulation of asset identification records, misrepresentation of improperly converted assets as in transit, and the kiting of cash collateral to use proceeds from borrowing on new, securitized assets to pay off loans made against old assets—another form of the Ponzi scheme.

Fraud on Auditors

The purpose of an independent audit is to determine whether financial statements do in fact present fairly the financial condition and results of operations of a company. If reported results contain accounting irregularities and do not comply with accounting standards, any intentional failure to disclose such a condition represents a fraud perpetrated on the auditors. This type of fraud has as its purposes obtaining from the auditors an unqualified audit opinion and keeping the auditors from knowing about and disclosing the accounting irregularities. Fraud on auditors typically includes some combination of the following elements:

- Misrepresentations by management and/or employees concerning the nature of transactions, the accounting applied, the absence of accounting irregularities—when in fact such accounting irregularities exist—and adequacy of disclosure
- Concealment of fraudulent transactions by means of falsification, alteration, and manipulation of documents and accounting records or in some cases, by keeping a separate set of books and records
- Subornation of collusion to defraud from among management and/or employees, taking the form of silence when in fact these persons have knowledge of the fraudulent activities but do not disclose their knowledge to the auditors, active participation in the fraud by corroborating misrepresentations and/or assisting in the falsification of books and records, and assistance in the circumvention of internal controls designed to prevent or detect fraud
- Collusion with third parties or other employees of the victim company, in which such parties are aware of irregular transactions but do nothing to prevent them and/or nothing to bring them to the attention of either their auditors or the counterparty's auditors
- Deceptions, including planning the fraud to take advantage of known or anticipated patterns of auditing—such as scope of testing or audit locations—and furnishing false information to auditors in response to their audit inquiries
- Destruction of evidential matter and/or withholding key documents such as side letters

Lying to an auditor can also result in criminal sanctions.

Corporate Frauds and Creative Accounting

Following is a table showing financial frauds that has happened in India:

No	Name of the Scam	Nature of Industry	Year	Fraud Perpetrators	Modus operandi	Money Involved (in crores)
1	Hashad Mehta	Capital Market and Asset Management	1992	Managing Director	Harshad Mehta led to rise in Stock Market by Trading in Shares at Premium	4000
2	C.R. Bhansali	Capital Market	1992-1996	Managing Director	Established Finance company and collected money from public and transfer money to Co. that never existed.	1200
3	Cobbler Scam	Co-operative Society	1995	Promoter	Availed loan of Crores of Rupees and created fictitious Co-Operative societies	600
4	Virendra Rastogi	Trading Company	1995-1996	CEO	Exported the bicycles by heavily invoicing the value of goods	43
5	Abdul Karim Telgi	Printing	2000	Promoter	Involved in Fake stamps Papers	171
6	UTI	Mutual Fund	2000	Chairman, Executive Director, Stockbroker	UTI issued 40000 Shares which were purchased for about Rs.3.33 Crores	32

7	Ketan Parekh	Capital Market	2001	Managing Director	Took loan of Rs. 250Crore from the Bank Whereas maximum limit was 1.5 crore	1500
8	Dinesh Dalmia	Information Technology	2001	Managing Director	Rs.1.30 crore shares are unlisted in Stock Exchange. Dalmia resorted ill legal ways to make money through partly paid up shares.	595
9	Satyam Computers	Information Technology	2009	Auditor, Director, Manager	Accounting Entries has been hugely inflated involving about Rs.100 Crores.	8000

Table. 1. Frauds in India

Creative accounting is a process whereby accountants use their knowledge of accounting rules to manipulate the figures reported in the accounts of business. It helps to maintain or boost the share price as well as boosting income as because of flexibility of rules and appraised report, a steady trend of growth in profit rather than to show volatile profits with a series of dramatic rises and falls which is achieved by creative accounting. It is totally legitimate only if, it is within the ramifications of the law and it achieves the company's ultimate goal of increasing stock values.

Following is a table showing list of companies using creative accounting:

Company	**Year**	**Nature of Creativity**
Satyam	1999-2009	Unethical manipulation of accounts and fraudulent transactions lead to the downfall of the company. Mr. Ramalinga Raju was fudging revenue figures every year and thus the gap between actual profit and book profit got widened every year. He raised fictitious bills for services that were never rendered. He also increased the cash and bank balances accordingly. Operating profits were artificially boosted from the actual ones. The Income Tax department is independently probing the accounting fraud in Satyam with a focus of tax deducted at source and BENAMI Deals.
Wipro Ltd.	1996-97 to 1999-2000	Transfer of land to stock-in-trade creating capital reserve to boost up net worth and to neutralize the effect on profit on reduction of land value.
Larsen & Toubro Ltd.	1999-2000 & 2001-02	Income recognition through transfer of loan liabilities at a lower consideration.
Bombay Dyeing and Manufacturing Company	2003-2004 & 2004-05	Creating provision for possible loss on firm purchase contract and subsequent write-back of such provision thereby converting operating losses into operating profit.
Hindustan Zinc Ltd	2003-04 & 2004-05	Reclassifying investments into tangible assets to blend the requirement of valuation of investments.
ONGC Ltd.	2004-2005	Capitalization of interest as well as other intangible assets to show fixed assets value upward and understating revenue expenses.
WorldCom	1999-2002	1. Booking ‘line costs’ (interconnection expenses with other telecommunication companies) as capital on the balance sheet instead of expenses. 2. Inflating revenues with bogus accounting entries from "corporate unallocated revenue accounts"

Enron	1996-2001	Enron report the entire value of each of its trades as revenue. Enron had used hundreds of SPEs to hide its debt. Enron’s balance sheet understated its liabilities, overstated its equity and profits. Enron's recorded assets and profits were inflated or even wholly fraudulent and nonexistent. In addition, its complex business model and unethical practices required that the company use accounting limitations to misrepresent earnings and modify the balance sheet to indicate favorable performance. Debts and losses were put into entities formed "offshore" that were not included in the company's financial statements.
Tyco International Ltd	1992-2002	10-million-dollar loan was totally forgiven by Tyco, and all interest was billed to the corporation. Kozlowski (CEO) was accused of tax evasion on some expensive art purchases, allegedly made with company funds. Kozlowski and Swartz were found guilty in 2005 of taking bonuses worth more than $120 million without the approval of Tyco's directors, abusing an employee loan program, and misrepresenting the company's financial condition to investors to boost the stock price, while selling $575 million in stock.

Creative accounting is totally legitimate and can be used if, only if, it is within the ramifications of the law and it achieves the company’s ultimate goal of increasing profits. Accounting practices which comply with GAAP and Accounting Standards are ethical. It is also something that can be used by any company irrespective of nature, size, location, etc. while accounting. There are ethical and unethical aspects of creative accounting.

Company	**Ethical (totally legitimate)**	**Unethical (not within the ramifications of law)**
Satyam		Mr. Ramalinga Raju said the manipulation of transaction started out small, and grew larger by the year, and later on turned into a big accounting scandal.

Wipro Ltd.		Creative accounting practices used by Wipro are unethical because the requirement of AS 10 and AS 2 have not been followed in spirit.
Larsen & Toubro Ltd.	Creative accounting practices used by L&T are justified because the requirement of AS is fulfilled, as holding company can transfer its liability to its subsidiary company.	
Bombay Dyeing and Manufacturing Company	Creative accounting practices used by Bombay Dyeing and Manufacturing company is ethical as it fulfills the requirements of AS-29. Accordingly, manager can make a provision for loss in the books of accounts, if loss is expected.	
Hindustan Zinc Ltd	Company changed the classification of particular investment to Intangible assets, is justified as the investment entitles the company to draw power regularly whereas such reclassification does not fulfill the requirement of AS-13 although the transaction is not unethical because it is justified according to AS-26. The auditor qualified the accounts for the years 2002-03, 2003-04 and 2004-05 in respect of the investment disclosed by the company as intangible assets	
ONGC Ltd.		Creative accounting practices used by ONGC Ltd. are not justified because it overstated its profits.
WorldCom		They classified over $3.8 billion in payments for Line costs as capital expenditures rather than current expenses. According to proper accounting principles line costs are to be treated as revenue expenses. Future expenses are accounted as Accrual.

Enron		Enron's recorded assets and profits were inflated or even wholly fraudulent and nonexistent. Enron transfer liability so that it would not appear in its accounts, allowing it to maintain a robust and generally increasing stock price
Tyco International Ltd		The SEC and Tyco International have indicted the former executives on charges of civil fraud and theft. Kozlowski and Schwartz are accused of giving themselves interest-free or low interest loans for personal purchases of property, jewelry, and other frivolities. According to the SEC, these loans were never approved or repaid.

Here one can say that large size companies have more scope for using creative accounting practices whereas small size companies have restricted scope of getting creative with their books of accounts. On the basis of selected companies all three foreign companies are large in size in comparison to Indian companies. For Example, Enron is a large size foreign company in comparison to all above mentioned Indian companies. So, scope for using creative accounting is large and wider for Enron in comparison to the selected Indian companies. It is also concluded that the foreign companies are using creative accounting more extensively and have been grossly unethical in comparison to Indian companies. Creative accounting practices used by Satyam, Wipro, ONGC, Enron, Tyco and WorldCom are unethical practices as these do not fulfill the requirements of AS, whereas the rest of the companies i.e. L&T, Hindustan Zinc Ltd. and Bombay Dyeing used creative accounting ethically for their benefit.

11. When and Why to Call in Forensic Accounting Investigators

The decision as to whether to bring in forensic accounting investigators is a judgment call. There is certainly no requirement in the accounting standards to do so. The benefits of consulting with forensic accounting investigators are just recently being evaluated and becoming better appreciated by auditing firms as well as the companies that use their services. If you were to ask investors and other stakeholders, they would be likely to say, “The more accountants sniffing around, the better.” But even forensic accounting investigators would tell you this is not necessarily true. The profession should strike a balance between auditing to obtain “reasonable assurance” that the financial statements are free of material error and doing so in a cost-effective manner. It makes little sense to impose a tremendous cost burden on society to pay for “fraud audits” at every company. Since most companies’ managements consist of honest people working for the good of the company and its stakeholders while complying with laws and regulations, conducting overly extensive and invasive audits does not make sound business sense. Yet the more that can be done to reduce the likelihood that a material fraud will occur and go undetected by the company or its auditors the better.

Auditors are not responsible for detecting counterfeit documents. Any respectable fraudster with access to a color printer or copier can create a false paper trail that would deceive even an experienced auditor. We’ve seen situations in which entire sets of documents had been created—in some cases, overnight—to deceive auditors. Audits involve the review of tens of thousands of documents by auditors who are not routinely trained or necessarily experienced in spotting altered or forged documents.

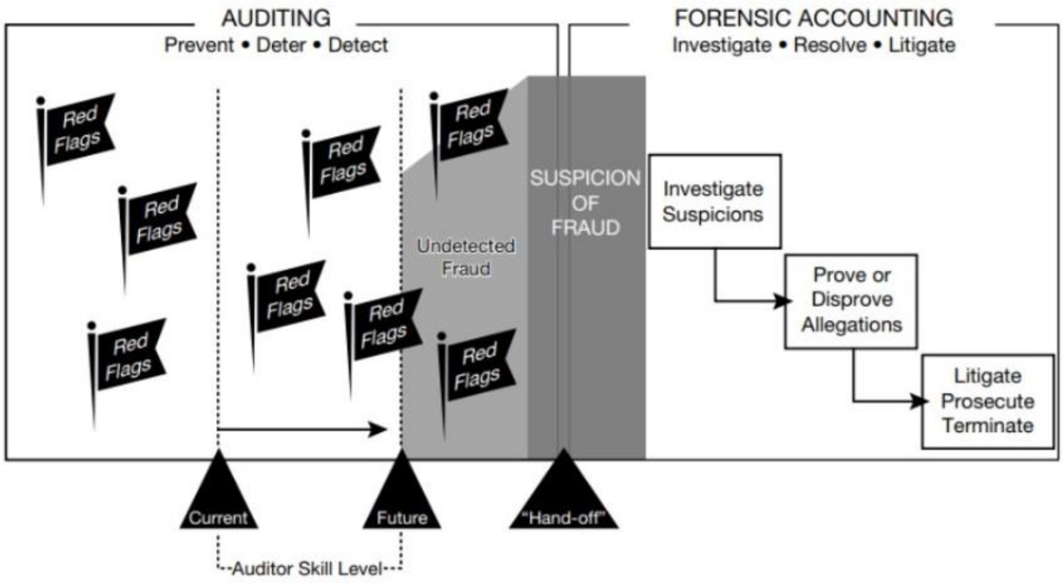

Fig. 6 The Red Flags of Possible Fraud: When to Hand Off the Forensic Accounting Investigation.

The auditor's professional standards do not hold auditors responsible for detection if a fraud is concealed by fraudulent documents. However, auditors armed with a healthy dose of skepticism will question the source from which they obtain information, recognizing that that information could be fraudulent.

Nothing short of repeated exposure to fraud can prepare one for effectively investigating frauds. Those who go on to become specialized forensic accounting investigators develop a keen sixth sense that supports the set of skills required for the resolution of complex fraud schemes.

When forensic accounting investigators launch a fraud investigation in an environment in which the perpetrator is unknown, they usually begin with interviews numerous enough to identify possible targets. During that process, they often hear such comments as: "Oh, it can't be Kathy. Kathy is one of our most loyal, long-term employees. She rarely takes time off, always works late, and helps others with their jobs. She's friendly, religious . . ." and so on.

Such a commentary on Kathy's work ethic and personality has no impact on the forensic accounting investigator's attitude, which must remain one of professional skepticism. The great majority of friendly, hardworking employees are honest; they are what they seem. However, most fraudsters also seem to be honest. The word con is a shortened form of the word confidence. Fraudsters seek to gain one's confidence, and the best of them are very good at it.

No book or school can adequately teach these realities to anyone. However, conceptual studies, missing from current college curricula, could provide a foundation for on-the-job learning and effectiveness. No standard requiring professional skepticism can substitute for actual experience with deceit. Providing training to surface more indicia of fraud and having forensic accounting investigators to call upon when such evidence surfaces are the best solutions to the problem. However, not all frauds will be detected or investigated to their ultimate resolution.

Many have suggested that the reason auditors did not detect in a timely manner the fraudulent schemes leading to some of the more significant corporate scandals was simply that the auditors' audit procedures had become predictable. There is no secret about what well-trained auditors examine in the course of an audit performed in accordance with regulatory standards. Once the audit leader has identified the risk areas in a financial statement prepared by company management, the focus and scope of the planned audit are defined easily enough. However, the relatively routine, predictable character of audit planning creates opportunities for fraud. When it is easy to determine the scope of an audit, it is often easy to plan a fraud around it.

12. TRIGGER POINTS OF FRAUD

Anonymous allegations of fraud, whether by letter, e-mail, hotline, or anonymous call. Whistle-blowers should be treated with utmost care. While seeking to take the allegations seriously, companies may wait too long to respond to whistle-blowers, who then believe they're not being taken seriously and who make a phone call to a third party or media. Every effort should be taken to respond to whistle-blowers immediately. Whistle-blowers should be encouraged to talk with a forensic accounting investigator who is trained in working with whistle-blowers. In such an interview, the forensic accounting investigator can form an opinion as to the probable validity of the allegations and can search for the reasons the individual has decided to come forward. The forensic accounting investigator knows there are occasions when people want revenge or attention and use the cover of whistle-blowing to satisfy their own needs. Although all whistle-blowers require immediate and thoughtful attention, there should be an attempt to test the allegations for validity—preferably, by face-to-face interview—before the decision is made to launch a full-scale investigation.

Discovery that a high-ranking official resigned due to known or possible illegal activities. Unless there is evidence indicating an irregularity, it is not usual that a forensic accounting investigator will be called in to perform an investigation. Although such an irregularity may emerge as an issue, the primary initial concern is that the executive may have acted improperly in other respects. A forensic accounting investigator may perform procedures—including interview and document examination and, very possibly, e-mail searches—to ascertain the likelihood of the allegations. If it is proved that the executive did in fact participate knowingly in illegal activities, the forensic accounting investigator usually recommends that the audit team review its audit programs to determine areas in which reliance was placed on the subject executive in the conduct of the audit.

A client identified as the target of an investigation by a law enforcement agency. Were the auditor to wait until the investigation is resolved before considering its implications for the audit, that would be a mistake. The length of time to complete an investigation is usually counted in months rather than weeks. In many instances, the company may not even know that the enforcement agency that launched the investigation has concluded it. Consider bringing in a forensic accounting investigator upon first learning of the investigation to discuss its implications.

An auditor who believes that intentionally misleading verbal information has been provided by the client, or that requested documents have been altered, or that documents are being withheld intentionally. Auditors may wish to confront the company personnel who they believe to be involved in the deception. If confronted, an individual may apologize profusely for creating such a misunderstanding and weave an explanation of some kind around the facts. The audit then continues, but the auditors may be left with the uneasy feeling that they have not received an honest response. Forensic accounting investigators use different techniques. For example, they may make use of indisputable facts about the suspected deception to see whether the individual lies or tells the truth in response to certain strategic questions.

Indications that a vendor may be fictitious. Fictitious anything should be a concern. One fictitious vendor may not seem all that important—and it may not be; it may represent a small, unintentional error. But it may also be the footprint of a fraud perpetrated by top management and concealed for years. It is advisable to call in forensic accountant investigators when suspicions about possible fictitious vendors arise—for the simple reason that the range of possibility stretches from an innocent recording error to a very large fraud.

Indications of improper accounting for revenue or expenses such as sales recorded before completed and final, goods shipped before a sale is final, revenue recorded while the customer is still owed future service or goods, or apparently false revenues recorded. The acceleration or outright fabrication of revenue and/or the deferral of expenses are among the most common financial statement frauds. While these issues may be investigated by auditors themselves, consultation with forensic accounting investigators may be helpful.

Other indications of fraud that may warrant consultation with a forensic accounting investigator include the following:

- Supplier refunds recorded as revenue
- Unbilled revenues or other accounts receivable being re-aged
- Bill-and-hold issues
- Recording vendor discounts as income
- Revenue recorded from self-dealing or asset exchanges
- Current expenses shifted into later periods
- Expenses improperly capitalized
- Liabilities concealed and not accrued
- Delayed asset write-offs
- Shifting expenses to a later period or advancing revenues

There are a number of other observable events that, while not necessarily indications of fraud, warrant appropriate warnings to the audit staff. The following conditions, either independently or in concert with other conditions, can be red flags of possible fraud. Where all of these conditions are concerned, auditors should proceed with a heightened level of professional skepticism in performing their planned audit procedures. Should indicia of fraud become evident, consultation with a forensic accounting specialist should be considered before proceeding beyond the scope of the audit plan.

Some of the observable events are as follows:

- Transactions that are not recorded in a complete or timely manner or that are recorded improperly as to amount, accounting period, classification, or entity policy
- Managers working below their level of authority
- Unsupported or unauthorized balances or transactions
- Last-minute adjustments that significantly affect financial results
- Evidence of employee access to systems and records inconsistent with the access necessary to perform authorized duties
- Significant unreconciled differences between control accounts and subsidiary records or between physical count and the related account balance that were not investigated and corrected on a timely basis
- Unusual transactions, by virtue of their nature, volume, or complexity, especially if such transactions occurred close to year-end
- Transactions not recorded in accordance with management's general or specific authorization
- Identification of important matters previously undisclosed by management
- Long outstanding accounts receivable balances
- High volumes of sales reimbursements and/or returns after year-end
- Suppliers' accounts with a high volume of debit and credit entries

Conflicting or missing evidential matter may also be a possible red flag suggesting fraud. These conditions include the following:

- Missing documents
- Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist
- Significant unexplained items on reconciliations
- Unusual documentary evidence such as handwritten alterations to documentation or handwritten documentation that is ordinarily electronically printed
- Inconsistent, vague, or implausible responses by management or employees arising from inquiries or analytic procedures
- Unusual discrepancies between the entity's records and confirmation replies
- Missing inventory or physical assets of significant magnitude
- Unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies
- Inability to produce evidence of key systems development and program change testing and implementation activities for current-year system changes and deployments
- Seriously incomplete or inadequate accounting records
- Contractual arrangements without apparent business purpose
- Unusual transactions with related parties
- Payments for services that appear excessive in relation to the services provided

Problematic or unusual occurrences between the auditor and the client may also be red flags of possible fraud. Such events include the following:

- Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence may be sought
- Undue time pressures imposed by management to resolve complex or contentious issues
- Complaints by management about the conduct of the audit or management intimidation of audit team members, particularly in connection with auditors' critical assessment of audit evidence or in the resolution of potential disagreements with management
- Unusual delays by the entity in providing requested information
- Tips or complaints to auditors about alleged fraud
- Unwillingness to facilitate auditor access to key electronic files for testing by means of computer-assisted audit techniques
- Denial of access to key information technology operations staff and facilities, including security, operations, and systems development personnel
- Frequent disputes with the current or predecessor auditors on accounting, auditing, or reporting matters
- Unreasonable demands on auditors, such as unreasonable time constraints regarding completion of the audit or issuance of the auditors' report— sometimes accompanied by warnings about the audit fee structure and expected duration
- Formal or informal restrictions on auditors that inappropriately limit access to people or information or that curtail the auditors' ability to communicate effectively with the board of directors or audit committee
- Domineering management behavior in dealing with auditors, especially when there are attempts to influence the scope of auditors' work or the selection or continuance of personnel assigned to or consulted on the audit engagement

- Client personnel displaying a hostile or unreasonable attitude toward audit personnel
- Client engaging in opinion shopping
- Managers' lying to auditors or evasion in response to audit inquiries to the point that dishonesty seems a likely diagnosis

13. Interviews and its importance in Investigation

Although interviews with witnesses in financial crimes differ from interviews with witnesses in other types of crimes, certain key interview techniques can help you as an investigator develop as much information as possible. In this chapter we have introduced you to some techniques that can aid you in both types of interviews. Our goal has been that you take two things away.

First, remember that, in general, the interview process is a dynamic relationship. The interaction between the investigator and the witness is the key to success of the interview. By employing such techniques as the use of cognitive interview skills you can increase your chances of building a better rapport. These techniques, though designed to enhance the recall of eyewitnesses to crimes, can be used effectively to enhance the recall of witnesses in financial crimes as well.

Second, preparation is the key to properly and effectively interviewing a financially knowledgeable witness. Although there is no magical list of questions that an investigator must ask, the skills you have developed reading the first section of this book should suggest a logical sequence and some general questions to use in certain financial crime interviews. Beyond that, there is nothing magical about interviewing financially bright people. Preparation will give you the edge, which will allow you to elicit the most detailed and accurate statement possible. “Be prepared” should be the motto of the financial crime interviewer, not just that of the Boy Scouts.

14. ANALYTIC PROCEDURES

Analytic procedures represent one of the most important detection techniques. Some may define these procedures as "evaluations of financial information made by a study of plausible relationships among both financial and non-financial data. . .. A basic premise underlying the application of analytic procedures is that plausible relationships among data may reasonably be expected to exist and continue in the absence of conditions to the contrary." Analytic procedures identify changes in amounts, ratios, trends, or relationships. They may also identify unusual transactions or events.

Analytic procedures are used throughout the audit process for three primary purposes:

- Preliminary analytic procedures are used to develop an understanding of the company and to direct attention to high-risk areas in determining the nature, timing, and extent of audit procedures.
- Substantive analytic procedures are used to obtain audit evidence to evaluate account balances.
- Final analytic procedures are used to assess the propriety of audit conclusions in an overall assessment of the presentation of the financial statement.

In the development of effective analytic procedures, the forensic accounting investigator should do the following four things: develop an expectation, define what result constitutes a significant difference from the expectation, compute the difference, and investigate the difference in order to draw appropriate conclusions.

Step 1. To develop an expectation, the practitioner must consider available information, including historical results, forecast amounts, industry trends, and general economic conditions. Simply expecting an account balance to be similar to historical results may be faulty logic. In light of this varied background information, ask yourself, "Does this make sense?" Realize, as well, that there may be still other environmental factors, which could help explain why consistency with prior years is not a reasonable expectation. Experience also shows that when management's only expectation is the achievement of budgeted income statement results, the pressure to meet that expectation can lead to fraudulent financial reporting that goes unnoticed precisely because the expectation is being met.

Step 2. To define what result constitutes a significant difference from the expectation, the forensic accounting investigator may consider the materiality of the account balance being analyzed, the risk of misstatement associated with that account balance, and even the controls surrounding that account balance. Each of these factors may have an impact on defining the significant difference. When considering the definition of a significant difference, the forensic accounting investigator should also consider the overall materiality of the financial statements, because a small fraudulent change in a large balance sheet item could have a material impact on the overall financial statements.

Step 3. To compute the difference, the forensic accounting investigator will prepare the actual mathematical analysis or analytic procedure. In the creation of the mathematical analysis, it is critical to consider the validity and completeness of the underlying information on which the analysis is based. Fraudulent transactions quite typically do not go through the normal checks-and-balances system. They are often included in or improperly excluded from "other" accounts, or they are on the corporate balance sheet as opposed to a division's. The inclusion or exclusion of a reconciling item between the subledgers and the general ledger is a common technique for concealment. The same can be said of reconciling items to outside sources such as between the general ledger and bank statements.

Step 4. To investigate the difference in order to draw appropriate conclusions, the forensic accounting investigator should consider seeking explanations from management concerning the differences noted. When possible, explanations from management should be corroborated by other evidence or corroborated by other company personnel not in the financial-reporting chain. For example, under a scenario of alleged inflation of revenue from transactions with certain new customers, if a significant increase in sales is explained by the fact that the company obtained a new customer during the period, the practitioner may request to see the customer contract and correspondence. The forensic accounting investigator may also consider speaking to the salesperson or customer service representative responsible for the new customer so as to better understand the relationship and verify the reality of the sale or sales and associated revenue. As you can see, a variety of approaches and techniques can be used depending on the situation.

Similarly, analytics may show that there is little fluctuation from prior years and that the company, subsidiary, or division is meeting or beating its budget or forecast. In situations in which management receives incentives based on achieving budgeted or forecast results, an analysis of annual changes may not be helpful. Analyzing quarterly or monthly changes may be more revealing as to whether financial information has been falsely presented and dressed up to meet expectations.

Applying disaggregated analytics when analysis is performed at the subsidiary or acquisition level can be a source of direct insight into allegations of wrongdoing and also identify areas for further review.

Analytics have revealed manipulations of financial data on a quarterly basis not only when management receives bonuses or incentives to meet and beat budget but also when there is an earnout agreement in place. For instance, the former management of recent acquisitions may be eligible to receive considerable payments if they meet a certain metric associated with earnings before interest and taxes or associated with earnings before interest, taxes, depreciation, and amortization, otherwise known as an earnout payment. In an actual case of this kind, analytics revealed that management was not meeting expectations to receive the earnout payment during the first two quarters. During the third quarter, the results were almost at expectation to receive the payment. In the fourth quarter, the results were achieved and management was paid millions based on the earnout-agreement provisions.

The auditors examined the calculation and found it to be calculated correctly. However, millions of dollars of false entries had escaped their attention during the audit because the debits were posted to accounts such as Intercompany, Fixed Assets, and Accounts Payable. In each instance, the entries were below the auditors' materiality threshold of $250,000. By the time of the audit, former management had resigned, their pockets lined with multimillion-dollar earnout payments.

Obviously, those earnout payments had not been earned in the spirit of the agreement. While the financial statement auditors may have applied analytics to the division in question, they did so annually and did not notice large, unexplained fluctuations. Analytics performed quarterly might have raised questions for review. Forensic accounting investigators applied this technique, and it led them to several bogus and unsupported general ledger entries posted at the end of the quarter, that had overstated the results by a material amount. With further probing, the forensic accounting investigators also learned that the financial statements for the acquisition had also been inflated, and thus the parent company had paid more for the subsidiary than it should have. The former owners and management profited by falsifying the financials on two occasions: once pre-acquisition, once post-acquisition.

Where was the due diligence team at the time of the acquisition? The parent company sent an internal team that was gung-ho to do the acquisition. The team was so gung-ho that due diligence was limited to a few top-level interviews and little analysis. Moral: it pays to do your homework and dive into the details. Analytic techniques, applied correctly, can often point the forensic accounting investigator in the right direction. The issue of when to apply the techniques depends on the facts and circumstances of an engagement. Some situations may dictate applying the techniques early and often, while in other situations, it may be more useful to apply the techniques at a disaggregated level, when more detailed financial information has been received and available.

15. ANALYTIC TECHNIQUES

As stated earlier, comparisons are made not only on account balances but also on financial relationships. Financial statement analysis generally falls into five categories: vertical analysis, horizontal analysis, ratio analysis, reasonableness testing, and analysis through data mining. These techniques for analyzing relationships are discussed as follows.

1. **Benford's Law:** It is a mathematical tool and is one of the various ways to determine whether variable under study is a case of unintentional errors or frauds. Use of parametric test called the Z test is carried to measure the significance of variance between two populations i.e. Benford's percentage numbers for first digit and observed percentage of first digit for a particular level of confidence. Benford's Law is not affected by scale invariance and is of help when there is no supporting document to prove the authenticity of transactions.
2. **Horizontal analysis**—that is, comparison of the current period's balances with those of prior periods. This technique calculates the percentage of change between the current-period balance, as well as prior-period balances, and a base period. Accounts that are increasing or decreasing at rates significantly higher or lower than the majority of the account balances—and especially compared with related accounts—might be subject to further scrutiny. For example, if sales increased 22 percent during the base period but if cost of goods sold increased only 9 percent, further analysis of both accounts might be warranted.

   Horizontal analysis is used to understand the percentage of change in individual financial statement items over a period of time. A base period, say, last year, is selected, and a percentage of change is calculated for other periods, say, this year, compared with the base period. Changes in certain line items, such as sales, should be the drivers for expected changes in cost of sales or selling expenses, for example. Looking at trends on a quarterly, monthly, or even weekly basis can also assist in identification of areas to be pursued. Disaggregating this monthly analysis further by business unit, geography, or customer may enable the practitioner to identify periods when revenue or expense trends are unusual. For example, monthly or weekly trends may indicate that a significant amount of the quarterly revenue is generated in the last week or month of the quarter with a particular customer.

3. **Vertical, or common-size, analysis**. This technique calculates each line item on a financial statement as a percentage of another line item. An income statement is common sized by showing each line item as a percentage of revenues. This is informative because many expenses, such as commissions or cost of goods sold, are directly dependent on the level of revenues. A balance sheet is common sized by showing each line item as a percentage of total assets—or total liabilities plus equity. These percentages are then compared against prior-period percentages or against industry or comparable company percentages.

   Vertical analysis (also referred to as common size analysis) compares elements of the financial statements with a common base item. For example, all elements of the income statement are expressed as a percentage of sales. These relationships are compared within each accounting period, and then the period under analysis can be compared with historical periods or industry information for context. Performing the same analysis on a disaggregated basis by business unit or by geography often gives the forensic accounting investigator a deeper insight into which business unit is driving an unusual relationship or whether one particular business unit is an outlier. The analysis can be further disaggregated through analysis of a particular financial statement line item by component. For example, cost of goods sold can be analyzed by business unit and by component: materials, labor, overhead, and variances. Again, this analysis may uncover an unusual trend in material costs, which would have been masked by opposite trends in other components of cost of goods sold. Vertical analysis can also be effective when a practitioner is performing analysis of the balance sheet. For example, comparing percentage of accounts receivable aging categories across business units may indicate cash collection deterioration in a particular business unit.

4. **Comparison of the detail of a total balance with similar detail for the preceding year(s).** This technique is based on analysis of the detail of a specific balance over time or at a point in time and comparison of it to similar detail from prior periods. If no significant changes in the client's operations have occurred in the current period, then much of the detail making up the totals in the financial statements might also remain unchanged. It is often possible to use this method to isolate information that needs further examination. An example might be a detailed analysis of the trade receivables account. Such an analysis could reveal that a significant increase in the number of customers occurred from one period to the next, with most of the new customers having balances below the typical materiality level for performing written confirmations. This might warrant further analysis.
5. **Ratios and other financial relationships**. Ratios reflect relevant information about a business by quantifying the relationship among selected items on financial statements. A company's ratios can be compared with ratios from a different period or periods, with

a competitor's ratios, and with an industry's ratios. Anomalies in the form of erratic or unexplained changes or differences from the industry may be investigated further. It is instructive to calculate liquidity, activity, leverage, and profitability ratios and figures. Ratio analysis assesses and measures the relationships among differing financial statement items and between these items and nonfinancial data. These ratios can be compared either on a historical basis, or on an industry basis, or against a benchmark. When unexpected changes occur, source documents and related accounts can be researched and examined in more detail. For example, in the retail industry, analyzing sales based on the square footage of each store location and comparing that information with other stores in the chain or with industry norms can be helpful in identifying stores that may not be performing as expected.

6. **Data Mining Techniques**: It is a set of assisted techniques designed to automatically mine large volumes of data for new, hidden or unexpected information or patterns. Data mining techniques are categorized in three ways: Discovery, Predictive modeling and Deviation and Link analysis. It discovers the usual knowledge or patterns in data, without a predefined idea or hypothesis about what the pattern may be i.e. without any prior knowledge of fraud. . It explains various affinities, association, trends and variations in the form of conditional logic. In predictive modeling, patterns discovered from the database are used to predict the outcome and to guess data for new value items. In Deviation analysis the norm is found first, and then those items are detected that deviate from the usual within a given threshold (to find anomalies by extracted patterns). Link discovery has emerged recently for detecting a suspicious pattern. It mostly uses

deterministic graphical techniques, Bayesian probabilistic casual networks. This method involves "pattern matching" algorithm to 'extract' any rare or suspicious cases.

16. COMPUTER-AIDED FORENSIC ACCOUNTING INVESTIGATION

Data-mining analysis might include all of the following:

- Scanning transaction listings
- Identifying gaps in check runs or shipping documents
- Identifying duplicate invoice numbers, payments, or payroll transactions to the same payee
- Matching return dates and credit memos to test for proper cutoff
- Comparing recent invoice prices with costs on the perpetual inventory records
- Filtering to identify all new suppliers, nonstandard journal entries, accounts under dispute, and the like
- Stratifying or grouping customer accounts by balance size or employees by overtime pay

Data-mining analytics are different from the other types of analytic procedures in that they are queries or searches performed within accounts or other client data to identify anomalous individual items, while the other types use aggregated financial information. What can be expected of data mining depends on the purpose of the procedure. For example, scanning a numerical sequence may bring to light certain gaps that merit investigation, while scanning payment amounts may yield evidence of duplicate payments. The expectation in searching for large and unusual items is based on the forensic accounting investigator's assessment of what constitutes normal. While some analytics such as a scan of closing or adjusting entries may be performed manually, others such as filters, duplicates, gaps, and sorts may require computer-assisted audit techniques using software packages like Audit Command Language, Access, or Excel.

Data mining uses software to assist the forensic accounting investigator in identifying and reviewing unusual data trends, patterns, and anomalies. Regardless of size, many of today's organizations maintain the majority of business transaction data in electronic formats. That is also true for many of the other primary sources of data potentially relevant to a forensic accounting investigator: customer and supplier information, product and price documentation, telephone logs, building security and access details, and employee data, to name but a few sources. The likelihood is high that most of the data the forensic accounting investigator is engaged to review will exist electronically, although previous chapters have made clear that forensic accounting investigators collate many different types of information, not all of which initially exists electronically.

As a result of the use of small-business management programs in smaller firms and enterprise-wide accounting packages in national or global firms, today's computer systems are vast warehouses containing data from finance, operations, marketing, and personnel. While small companies engage in hundreds or thousands of transactions, large-company transactions number in the tens or hundreds of millions, even billions. Given such volume, relying exclusively on manual investigation skills (without using computer aided techniques) to uncover suspect transactions is too expensive and likely to overlook key data. Within those thousands or millions of records could be fraudulent activity that may remain hidden unless the right tools and know-how are applied to bring the issues to light.

Data analysis is often the fastest and most effective tool at the forensic accounting investigator's disposal for gathering much of the evidential material needed to support findings. Much of the data, particularly the non-accounting data, is never used directly by the organization in question, but any of it may hold the key to an investigation. In cases in which the forensic accounting investigator has been engaged on the basis of a suspicion or an as yet unsubstantiated allegation, the results of data mining may provide the forensic accounting team with that all-important place to start. Auditors too often use software tools—some of them generic or homegrown— to query accounting systems, gain assurance with respect to data integrity, and in some instances, identify so-called unusual transactions.

BENEFITS AND PITFALLS

Using software applications and understanding their capabilities from basic to advanced can bring rapid and powerful results to the successive phases of an investigation. However, to be most efficient, users must know how and why to employ such tools. One cannot assume that all forensic accounting investigators, experienced or otherwise, are skilled users of software as an investigatory tool. In lieu of using software, many experienced forensic accounting investigators continue to rely on interview techniques and document review. However, once forensic accounting investigators have been introduced to advanced software tools, they often find that depending on the situation, they are likely to bring added value to clients through increased efficiency.

Many types of software applications and an ever-increasing array of new products and versions are available. The vast range of software offerings argues against any attempt to provide a comprehensive listing of such tools. It is possible, however, to describe both the benefits and the pitfalls of requesting, obtaining, and analyzing computerized information. The benefits will make clear why data mining should be viewed as an integral part of the investigation process. The pitfalls will help steer the reader away from the more common mistakes.

BENEFITS

- The forensic accounting investigator is able to analyze a large number of transactions, identify trends, spot documents that need further review, and gain initial insights without waiting for the cumbersome process of collecting documents by traditional means.
- Data mining is often a more cost-effective and more comprehensive approach than hard-copy document review.
- Computerized information can assist in providing reasonableness checks of findings based on documents, especially in situations in which document sets may be incomplete. It also enables the investigating team to check 100 percent of an entity's transactions for certain characteristics such as date, time, dollar amount, approvals, and payee depending on the nature of the computer record.
- With data analysis linked to presentation software, findings can be more clearly summarized for board, audit committee, or management presentations.

Fraudsters necessarily make use of the computer systems that corporations depend on for day-to-day operations. Tech-savvy fraudsters often make use of email and instant messaging, they access networks, they create and manipulate all sorts of files, and they work with databases and general ledger systems. They may also use printing, scanning, and fax technology to create all types of fictitious documents, many of which have the look and feel of the real thing. In many cases, these traditional frauds, con games, and embezzlement schemes are also cybercrimes. In other cases, a fraudster may simply use computer networks just as fraudsters in the past used telephones and filing cabinets. But there is a difference. Computer networks often provide better audit trails and information about what was done by a would-be fraudster than the paper-based record-keeping systems that have been replaced in the past 25 years. Understanding the tools and techniques of forensic technology investigations provides a wealth of information to review that would be otherwise unavailable or at least more difficult to obtain. In investigations, having more information is a key asset.

17. THE FUTURE OF FORENSIC ACCOUNTING INVESTIGATION NEW TOOLS

There can be no doubt that the electronic tools available to forensic accounting investigators will continue to ramify and improve. As in many other fields, the Internet has created communities of interest at Web sites where participants can share information about new tools and the use of existing tools.

One of the most interesting trends is toward improving on existing software applications by developing proprietary applications of far greater capability than those offered commercially. For example, while powerful data-mining software is commercially available, it may not always be capable of extremely high volume, data-mining exercises. Forensic accounting investigators involved in such projects may need to ask their technology coworkers to adapt existing programs to meet the demands of such large-scale projects. For projects of average scope, however, commercially available software is virtually certain to keep improving and to be up to the challenge.

EDUCATION AND TRAINING: TO BETTER SUPPORT THE NEW DISCIPLINE

We see signs of a positive trend: in the future, an increasing number of undergraduate and graduate programs are likely to offer courses in forensic accounting investigation. For courses to be more than conceptual overviews, they should be taught by those who have performed hands-on work in actual investigations. This need suggests the value of crossover teaching arrangements that have, in fact, already been piloted with success at a handful of U.S. institutions. Working forensic accounting investigators often prove to be enthusiastically willing to teach, and team teaching with resident academics may be the most effective formula.

Even guest appearances by experienced forensic accounting investigators would be gains in the context of ongoing courses on audit methods. Seasoned forensic accounting investigators should find a place in universities.

Firms with forensic accounting investigation capabilities may be persuaded to fund tours of duty for academics to join their forensic accounting investigation teams, so that those individuals can experience the attitudes and methods and the uncertainties and problem solving of the real world of forensic accounting. As well, we would expect—and we certainly hope for—a trend toward investment in education on the part of major firms with forensic accounting investigation capabilities either by their funding of college programs or by their funding of chairs in forensic accounting investigation.

CHANGING CORPORATE ENVIRONMENT

In many cases, managements and boards of directors are becoming much more aware of their obligations, new and long-standing, to deter and combat fraud within their organizations. Many audit committees are listening; they are meeting more frequently and more probingly with auditors, and they are requesting additional investigation of alleged frauds when that seems to be the prudent course. Some audit committees are adopting the loose-thread approach to evidence of possible fraud, which we have recommended in this book: where there are small indicia of fraud—small threads out of place—those audit committees are interested in looking more closely to discover whether something more important and pervasive may be underlying. The professional standards governing the work of those committees now require further inquiry when evidence of possible fraudulent behavior surfaces, even if the amounts are likely to be quantitatively immaterial. The CEO and chief financial officer (CFO) are specifically charged with certifying the financial statements, and they must report to the external auditors and the audit committee any incidence of fraudulent behavior committed by those involved in the internal controls over financial reporting.

we see a positive tendency on the part of companies to prepare better in advance through policies and procedures that will address allegations of fraud without delay, should they arise. Companies are learning not to wait until fraud is detected to develop an operating plan.

Future of forensic Accounting Investigation: Increasing Globally

International forensic accounting investigation assignments can be among the most challenging, intricate, and interesting. The trend is toward more of them. Even without the benefit of a crystal ball, it is evident that well-trained and experienced forensic accounting investigators from many parts of the world should find that their skills are needed and valued both at home and abroad.

The field of forensic accounting investigation is advancing in worldwide, with more sophisticated challenges to address and resolve and with more sophisticated tools at hand. The field will be, and deserves to be, a gathering place for outstanding auditors who have looked at the conceptual and practical challenges of forensic accounting investigation and looked also at the personal demands of the field, which are not small. In light of everything those auditors have seen, they recognize a strong affinity, and they seek the training and experience that will make them capable practitioners. They belong to the profession. The profession will repay them many times over, not only with sound careers but also with the knowledge that they are making a unique contribution to the integrity and strength of markets on which all economies depend. Critical to a company's success in addressing the very real threat of financial fraud are knowledgeable auditors, directors, and management working effectively with skilled and experienced forensic accounting investigators.

18. CONCLUSION

India is one of the fastest growing economies of the world. It is at more risk of frauds as the rules and regulations prevalent in country are not able to catch up with the changing circumstances. Repetition of fraud cases where high profile and trusted people are involved has raised the demand for improving the current system of checks and controls. Forensic Accounting is more into news these days as there is an increase in white-collar crimes and financial frauds in the world.

It has been observed that the financial scams in India are unbridled due to lack of tringent surveillance authority. If we consider the quantum of loses from these scams. They are an eye opener. Satyam's scam was a fraud involving about Rs. 8000 crores. Harshad Mehta triggered a securities scam diverting funds to the tune of Rs. 4000 crores. Ketan Pareskh followed Hrashad Mehta's footsteps to swindle crores of rupees from banks. India has already faced substantial losses due to rapid increase in white-collar crimes and the belief that our law enforcement agencies do not have sufficient expertise or the time needed to uncover frauds. Moreover, the Forensic Accounting is in an infancy state in India. It is still an untrodden area in India.

The immediate landmark creation is "Forensic Research Foundation”. They provide support for investigation of fraud. They publish one bimonthly journal named as "White Crimes". It relates to forensic and economic crimes. Another International organization named as KPNG has set up an investigation detection centre in India. Networks Limited, a Delhi based organization, working in the similar field, they are also trying to innovate ways and means to detect financial irregularities and crimes in India. Serious investigation Fraud Offices (SIFO), has been established in India for the same reason, i.e. Detection and prevention of economic irregularities and crimes. The collaborations should be initiated with International agencies and institutes working in the area of forensic accounting It is a good way to contribute to the body of knowledge and learn from the experience of others.

But there are very few professionals in India who are pursuing a career in Forensic accounting. One of the reasons may be that they are not aware about the scope and prospects of this profession in future. Other reason may be that people are not confident enough to take it as a full-time occupation due to lack of formal education and training in this field. Forensic accounting has grown up as an independent area and it can be pursued as a full-time profession. It is also expected that forensic accounting will be one of the top 20 most sought-after jobs in the world in the next decade. Forensic Accounting should be introduced as a subject in education institutions at various levels to fulfil the gap in supply of forensic accountants through education and training, it is required to identify the skill set required in a competent forensic accountant.

19. Bibliography

- https://elearning.scranton.edu/resource/business-leadership/what-is-forensic-accounting
- https://www.online-accounting-schools.org/faq/what-is-forensic-accounting/
- https://www.cfoedge.com/blog/controls/whats-the-difference-between-financial-accounting-forensic-accounting/
- https://www.online-accounting-schools.org/faq/what-is-forensic-accounting/
- https://elearning.scranton.edu/resource/business-leadership/what-is-forensic-accounting
- https://www.acfe.com/rttn2016/schemes/occupational.aspx#:~:text=As%20reflected%20in%20the%20graphic,corruption%2C%20and%20financial%20statement%20fraud.
- Forensic Accounting and Fraud Investigation by Howard Silverstone, Stephen Pedneault, Michael Sheetz, Frank Rudewicz
- Forensic Accounting and Fraud Investigation for Non-expert by Haward Silverstone and Michael Sheetz
- Essentials of forensic accounting by Carl pacini, Michael A Crain, George R Young and William S Hopwood
- Forensic Accounting for Dummies by Frimettee Kass-Shraibman, Vijay S Sampath
- Application of Forensic Accounting to Investigate Scams in India By Sana Moid
- Forensic Accounting: An Emerging Approach to Deal with Corporate Frauds in India By Shirish Mishra and Gurbir Singh
- Indian Journal of Accounting Dec 2013