# Forensic Accounting and Fraud Examination

## DEACC210

Edited by:
Dr. Nancy

LOVELY PROFESSIONAL UNIVERSITY


# Forensic Accounting and Fraud Examination

Edited By
Dr. Nancy

# Content

Dr. Razia Sehdev, Lovely Professional university

# Unit 01: Introduction to Forensic Accounting and Fraud Examination

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the meaning of forensic accounting.
- review the characteristics of forensic accounting.
- illustrate the types and applications of forensic accounting.
- examine the role of forensic accounting in litigation support and criminal investigation.
- explain the scope and importance of forensic accounting.
- illustrate the techniques adopted in forensic accounting.
- appraise the evolution of forensic accounting.

- examine the meaning and role of a forensic accountant.
- explain the characteristics and qualities of a forensic accountant.
- illustrate the skills required to be a forensic accountant.
- appraise the meaning and importance of forensic audit.
- review the meaning and role of the forensic auditor.
- explain the qualitative characteristics of a forensic auditor.
- compare forensic audit and financial audit.
- compare a forensic accountant and a forensic auditor.
- review the role of forensic accounting and forensic experts to detect frauds and felonies done by an organization or individual.

## Introduction

In recent years, the growing globalization&digitalization have changed the business environment for a better purpose. However, the incidents of financial crimes and fraud have also increased.

Large organizations usually maintain a distinct department of in-house accountants who oversee all business activities and endeavour to minimize financial irregularities or crimes. Still, new and innovative fraudulent activities can only be detectedafter an in-depth analysis of all business financial records.

The investigation of fraud or financial irregularities by performing extremely detailed research and business information analysis is forensic accounting. Forensic accountants are generally hired to prepare for claims related to litigation, insurance claims, divorces, insolvency, embezzlement, skimming, fraud, and any type of financial theft.

Forensic accounting is not a new specialized area of accounting. The skill set and activities encompassing forensic accounting have been around for quite a while, although it was not necessarily always called forensic accounting.

Forensic accounting became common parlance when the massive financial and accounting scandals involving Enron and WorldCom came into the limelight. Such scams elevated the need for forensic accountants in various industries who can prevent and investigate frauds with their expertise in accounting and auditing, and technical skills.

## 1.1 Forensic Accounting: Meaning and Definition

### Forensic Accounting: Meaning

When you ask any two or more practising forensic accountants to define what forensic accounting is, you are likely to get different answers. Each may be accurate, and their responses likely will be similar. However,there is still no consistent answer recited by everyone who practices in this specialized area of accounting. The responses will depend mainly on the background, experience, and areas of practice of each forensic accountant.

It involves using accounting skills to investigate financial crimes such as money laundering, embezzlement, tax fraud, etc., and to analyze financial information for use in legal proceedings.

In other words, Forensic accounting is the investigation of fraud or financial misrepresentation, or manipulation by performing extremely detailed research and analysis of financial information. It utilizes accounting, auditing, and investigative skills to examine the finances of an individual or business. It provides an accounting analysis suitable to be used in legal proceedings.Forensic accountants are trained to look beyond the numbers and deal with the business reality of a situation. It is frequently used in fraud and embezzlement cases to explain the nature of a financial crime in court. They are often hired to prepare for litigationrelated to insurance claims, insolvency, divorces, embezzlement, fraud, skimming, and any type of financial theft. They conduct an in-depth analysis of financial data. They document the entire investigation and report findings to a court of law.

**Did You Know?**

What is Skimming fraud?

Skimming fraud is a white-collar crime involving taking a business's cash before entering it into the accounting system. Skimming is an "off-book" fraud because the cash theft occurred before it was entered into the bookkeeping system. Thus, it is never reported on the company's accounting records.

Forensic accounting services generally involve the application of specialized knowledge and investigative skills possessed by CPAs to collect, analyze, and evaluate evidential matter and to interpret and communicate findings in the courtroom, boardroom, or another legal or administrative venue. These resources are intended to assist practitioners in competently performing these duties while staying current on issues impacting their daily practice.More simply, in the context of litigation, the term forensic means suitable for use in a court of law.

--- AICPA

### Forensic Accounting: Definition

"Forensic accounting 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".

- Hopwood, Leiner, and Young

Forensic Accounting and Fraud Examination by Kranacher, Riley, and Wells define financial forensics similarly, as follows:

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 recognize the role of the financial forensic professional as an expert or consultant.

2. Investigative services use 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.

## 1.2 Forensic Accounting: Key Characteristics

The prime characteristics of forensic accounting are listed below:

- Forensic accounting combines accounting, auditing, and investigative skills or techniques to discover financial crimes and assist in legal matters or proceedings.
- It applies scientific techniques and accounting principles to detect fraudulent activities.
- It entails an accounting analysis that can reveal possible frauds suited for presenting in courts.
- Accounting analysis produced by Forensic accounting should form the basis for discussion, debate, and dispute resolution.
- One of the essential functions of forensic accounting is to explain the nature of a financial crime to the courts.
- It involves the detection of the application of embezzled funds, asset identification, asset recovery, and due diligence reviews.
- It is sometimes called investigative accounting,which combines accounting and auditing with information technology.
- It includes three main areas: litigation support, criminal investigation, and dispute resolution.

- The insurance industry highly applies it to establish damages from claims.
- It is a widely applied accounting discipline that resolves financial conspiracies—money laundering, bankruptcy, embezzlement, insurance claims, securities fraud, asset misappropriation, tax evasion, divorces, family disputes, financial scams, and debt defaults.
- A single person cannot execute forensic processes. Instead, it is carried out by a structured team of professionals and experts like Certified Public Accountants (CPAs), Chartered Accountants (CAs, Forensic Accountants, Management and Cost Accountants, Auditors, etc.
- Forensic experts probe financial information and other relevant details of a company or an individual to detect fraud or crime.
- They collect evidence and study financial crimes. They discover legal violations and prove them in a court of law.
- Financial experts apply their expertise in accounting, law, investigative auditing, and criminology to unveil fraud and present proof in court.

## 1.3 Forensic Accounting: Types and Applications

Various types of forensic accounting can take place. Here are some of the most common examples:

- Business fraud investigation
- Tax fraud
- Securities fraud
- Asset Misappropriation or Hidden Assets
- Partnership shareholding dispute
- Insurance claims
- Economic losses and Bankruptcy
- Money laundering
- Matrimonial cases like Divorce proceedings
- Financial theft (customers, employees, or outsiders)
- Economic damages (various types of lawsuits to recover damages)
- Corporate valuation disputes
- Professional negligence claims
- Privacy information
- Personal Insurance
- M&A related lawsuits

**Business fraud investigation**

Business investigations comprise asset identification, asset recovery, due diligence reviews, tracing misappropriation, forensic intelligence, and suspect interviews. Forensic accountants strategize intelligence measures and identify offenders. These investigations require a detailed review of the documents.

**Tax Fraud**

Businesses and individuals often falsify income and other financial information to reduce tax liabilities.Forensic expertsidentifysuch tax evasion.

**Securities Fraud**

Misrepresentation of investments, commodities, and stocks is the most common white-collar crime. Late-day trading, pump and dump schemes, pyramid schemes, and Ponzi schemes are felonies. Forensic experts assist in detecting such securities frauds.

**Asset Misappropriation or Hidden Assets**

Individuals and companies often hide assets from tax authorities and other regulatory bodies. Forensic experts detect asset misappropriations—property theft, embezzlement, and payroll fraud.

**Partnership and Shareholding Dispute**

Forensic experts also examine compensations and benefits received by shareholders or partners. The investigation involves detailed scrutiny of accounting and financial records to quantify the issues brought out in the conflict.

**Insurance Claims**

Forensic expertsquantify economic damages in vehicular accidents and medical negligence cases. They review insurance policies, coverage issues, claim settlements, and the calculation of potential losses. On behalf of insurance companies and policyholders, they investigate property losses, business losses, employee fidelity claims, and similar lawsuits.

**Economic Losses and Bankruptcy**

Business losses typically include breach of contract, construction claims, trademark infringements, patent infringements, product liability claims, and non-compete agreement breaches. Forensic experts probe into the terms and conditions of the circumstances leading up to the disputes. They quantify the losses. In addition, forensic experts carry out recovery procedures in bankruptcy cases.

**Money Laundering**

Forensic professionals identify illegitimate sources of money – money laundering practices and undisclosed bank accounts.

**Did You Know?**

What is Money Laundering?

Money laundering is the concealment of the origins of illegally obtained money, typically through transfers involving foreign banks or legitimate businesses.

Matrimonial cases like Divorce proceedings and Marital and Family Disputes

After quantifying losses, forensic accountants assess financial compensation for divorces, property, and family disputes. They quantify payment for alimony and child support. For family and property disputes, forensic accountants execute property distribution.

## Forensic Accounting: Applications as per AICPA

The American Institute of Certified Public Accountants (AICPA) announced a new credential for those CPAs focusing on forensic accounting and litigation support. Certified in Financial Forensics (CFF) credential became effective in September 2010. The AICPA defined the field of forensic accounting to include a fundamental basis of knowledge and specific practice areas or applications for forensic accounting.

### Fundamental Knowledge

- Laws, Courts, and Dispute Resolution
- Planning and Preparation
- Information Gathering and Preserving
- Discovery
- Reporting, Experts, and Testimony

### Specialized Forensic Knowledge

- Bankruptcy, Insolvency, and Reorganization
- Computer Forensic Analysis
- Economic Damages Calculations
- Family Law
- Financial Statement Misrepresentation

### Bankruptcy, Insolvency, and Reorganization

Forensic expertscan be hired on the debtor's behalf in case of Bankruptcy. Their work may be to assist the trustee in managing the financial affairs, searching for hidden assets, identifying pre-bankruptcy transfers, recovering funds and assets to satisfy creditor's claims, or performing business valuations to resolve the bankruptcy filing.

Forensic expertscan also be retained by creditors seeking to determine whether additional assets exist or whether any payments were made immediately before filing.

Unfortunately, bankruptcy fraud is common, and the forensic expert's role often works to corroborate and support the disclosures and claims under bankruptcy fraud.

### Computer Forensic Analysis

Two main applications for computer forensics are the preservation and recovery of electronic information for evidence purposes and electronic discovery for litigation support. With the advent of digitization, more and more transactions are being completed electronically within both business and social settings.Valuable information and evidence can be found in files maintained in places beyond the traditional computer and server hard drives. As technology moves toward "cloud" computing, whereby information is kept and accessed through the Internet, the physical location of the data will exist outside of the business and likely outside of the country.

The latest gadgets, including Blackberries, iPhones, iPads, laptops, netbooks, and cell phones, can all connect to the Internet and transmit electronic information. Knowing the types of electronic information that may exist, what form and format it possesses, where it could be located and accessed, and, most importantly, how to gain access to it could be the most significant factor in general litigation or proving your case.

### Economic Damage Calculations

Damages are a crucial component of every lawsuit. If a party believes it has been harmed or wronged but cannot identify or prove itsuffered damages, the likelihood of the party prevailing in litigation is not good.Two key terms for this area of litigation are causation and damages. Causation means the actions or inactions of one party that caused the injury or loss of the other party. Damages refer to the calculated loss suffered as a result of causation.

Forensic accountants are called upon to calculate losses in many contexts, including lost earnings, lost profits, lost business, and the physical loss of property (e.g., fire, flood, theft).

### Family Law

Forensic expertscan have several roles within marital dissolution (divorce and post-divorce) engagements, starting with the role of a strategist working with counsel and the client before the divorce is even filed.The forensic accountant may work with counsel to uncover hidden or undisclosed sources of income or assets that should have been appropriately included on a party's financial affidavit. Earnings and expenses of each party, along with earning potential, will come into play in calculating alimony and child support.

### Financial Statement Misrepresentation

This area would entail the forensic accountant being retained to examine the financial statements and disclosures of publicly traded and privately held entities and organizations to determine whether the financial statements correctly reported the balances, results, and required disclosures.

### Fraud Prevention, Detection, and Response

An organization can hire forensic accountants to evaluate its systems of internal controls, financial policies proactively, and accounting procedures before any thefts are identified, as well as to seek indications of fraud within specific areas even when no "red flags" or manifestations of fraud exist.

### Business Valuation

Forensic accountants are called upon to conduct business valuations within several contexts. The valuation may be required for dividing assets in a divorce, as discussed earlier, or maybe part of some other type of litigation, such as a shareholder dispute.

**Caution**

Litigation is the process used to resolve a lawsuit. A lawsuit is a specific legal action wherein the plaintiff files a complaint with the court. Litigation is the series of steps before, during, and after a lawsuit is filed. This involves studying the case and sending demand letters to the defendant. Then the defendant is given time to respond. During litigation, the defendant is served a summons or complaint that requires legal action, a lawsuit.Afterwards, litigation typically ends with a verdict, the result of a court case, in which a judge orders compensation, damages, or something else

. **Note:**Even after a lawsuit is resolved, the litigation process can continue.

**Example:** M/S Cameo filed a lawsuit against M/S Zymia. M/s Cameo lost the case. Thus, itwas left dissatisfied with the resolution of the case. In this scenario, it could file for an appeal or negotiation with a higher court. This causes the litigation to resume.

## 1.4 Role of Forensic Accounting in Litigation Support

Forensic accounting and its experts,viz. forensic accountants,and forensic auditors,are essential because they have a unique skill set, are trained in the investigation and expertise in accounting records,and their evidence plays a significant role in judicial decision-making. This job is quite different from the auditor and cannot substitute by them.

The auditor performs its testing in the accounting records against accounting standards like AS, Ind As, US GAAP, or IFRS. Their responsibility is not to investigate and quantify the fraud that happens in the company, and also, the evidence found by the auditor might not be used by the court. However, the evidence found by forensic accounting could be used by the court as expert evidence.

Sometimes, the lawyer or court needs someone with expertise in accounting and investigation to examine and produce reports on accounting-related areas. These people have exceptional skills in accounting and investigation. As they are independentof all parties, thus their report is considered more reliable and bearsno objection from all the parties.A forensic accounting expert checks the damages experienced by the parties suffered in legal disputes. They can also help settle conflicts, even before they reach the courtroom. If a conflict enters the courtroom, the forensic accounting professional can give evidence as an expert witness.

**Notes:** Forensic accounting is utilized in litigation when quantification of damages is needed. Parties involved in legal disputes use the quantifications to assist in resolving disputes via settlements or court decisions.

**Example:** Suppose there is a conflict between Simba, an employee of Mango Tree, a restaurant chain,due to compensation and benefit disputes. The forensic accountant may work as an expert witness if the disagreement escalates to a court decision.

The following forensic accounting reportscan be prepared to support the differentlitigations in court:

- **Produce the company's income statement:** This is simply figuring out how much profit or loss is earned or incurred by the company, or its specific branch, brand, and project.
- **Prepare Lost earnings/wages reports related to loss of profits of the employee:** The best example for this point is if the employee sues their employer for wrongful dismissal and the court wants to figure out what the subsequent loss of this dismissed for the employee.
- **Investigation of parties' breach of contract:** This typically happens in daily business activities. Such examination will study the detail of the terms of the contract and the way how parties will perform their contractual obligations. The report who respect, disrespect,

contractual obligations,and loss resulting from the breach of contract will be calculated and presented to the court.

- **Death report:** A wrongful death report results from an investigation related to death, whether criminal or civil.
- **Patent and copyright violation reports.**
- **Fraud Investigation report:** This report is used by the court and lawyer to determine the amount of actual loss andthe accused parties responsible for committing fraud.
- **Business diminution report**
- **Professional malpractice report**
- **Wrongful termination report**
- **Expert Witness Testimony**

**Did You Know?**

What is an expert witness testimony?

A Forensic Accountant could also be the expert witness testimony on how the Fraud is committed, who committed the Fraud, and the amount of loss. Such a witness will be part of the court's decision-making. They could also be witnessed over the accounting records related toashareholder dispute.

A forensic accounting expert measures the damages experienced by the parties implicated in legal disputes and can aid in setting conflicts, even before it reaches the courtroom. If a conflict reaches the courtroom, the forensic accounting professional could give evidence as an expert witness.

## 1.5 Forensic Accounting for Criminal Investigation/Fact-Finding Services

When we talk about the investigation from a forensic accounting perspective, it revolves around criminal or fraud investigation.Fraud is a significant expense for the company and is hardly investigated and eliminated. The fraud investigation could be performed in many corporate, public, or private organizations. The investigation could also beconducted in many different areas like Fraud over financial reporting, fraud over the entities' assets, and employee fraud investigation. Employee fraud investigation is the most demandedservice of forensic accountants.

**Examples:** Fraud over salaries, inventories, fixed assets, or cash collections.

In this case, forensic accounting could provide the investigation services and figure out how much the suffered loss for specifiedinstances. A forensic accountant would determine whether illegal matters or financial crimes such as employeetheft, securities embezzlement (including tampering and distortion of financial accounts), identity theft, manipulation of financial records, and insurance fraud have taken place.The investigation report could also include the cause of fraud and the mechanism of the scam. Assessment of the likelihood of criminal intent could also be part of the report.

**Caution:** Forensic accounting is often brought in complex and high-profile financial crimes.

- Harshad Mehta Securities Fraud
- Satyam Scandal
- PNB Fraud
- 2G spectrum fraud etc.

The scope and mechanisms of these frauds are understood today because forensic accountants dissected the schemes and made them understandable to the court and general public.

- Forensic accountants may also assist in identifying hidden assets in divorce cases or provide their services for other civil matters such as breach of contracts, tort, disagreements relating to company acquisitions, breaches of warranty, or business valuation disputes.
- Forensic accounting assignments may include investigating construction claims, expropriations, product liability claims, or trademark or patent infringements. And, if all that wasn't enough, forensic accounting may also be used to determine the economic results of the breach of a nondisclosure or non-compete agreement.
- The insurance industry often uses forensic accounting. In this capacity, a forensic accountant may be asked to quantify the economic damages arising from a vehicle accident, a case of medical malpractice, or some other allied claim.The forensic accountant can help both policyholders and insurers prepare and review the claim based on the term and conditions that cover the insurance policies. He might work closely with the accounting assurance team that knows clearly about financial loss. In some cases, this service also allows the insurance company to review the claim submitted by the policyholder to quantify the claim amounts.

## 1.6 Forensic Accounting: Scope

Forensic accounting is generally described as accounting that is used for legal purposes.The scope of forensic accounting is to:

- Look for evidence of significant development in the accounting and financial systems.
- Design accounting processes for verifying relevant premises and data. A forensic accounting orientation also calls for skills in identifying possible fraud.
- Perform audit-type processes on a routine schedule to reduce transaction processing risks.
- Cover a broad range of businesses and locations that require routine or continuous surveillance of all transaction processing systems.
- Thefollowing are a few cases and institutional bodieswhich demand the use of Forensic accountants' services:
  - ✓ Insolvency cases
  - ✓ Bank Forensic Audits
  - ✓ Economic Offenses Wings
  - ✓ Securities Exchange Board of India
  - ✓ Serious Fraud Investigation Office

## 1.7 Forensic Accounting: Importance

The relevance of forensic accounting in an organization is as follows:

- Assessing working transactions for compliance with basic operating processes and agreements.
- They thoroughly scrutinize and examine financial payment dealings in the accounting system to decide if they are standard or beyond company policy.
- It assessesconventional ledger and financial reporting system transactions for likely unlawful tampering or falsification of information or accounts and its consequences on the ensuing financial statements.
- Analyzing warranty requests or returns for practices of fraudulence or misuse.
- Assisting in estimating the economic damages and the insurance demands arising from catastrophes such as fires or other natural setbacks.
- Assessing or affirming business rating in consolidations and accomplishments.

## 1.8 Forensic Accounting: Techniques

The techniques that can be adopted in forensic accounting are as follows:

- Reviewing public documents and performing background checks
- Conducting interviews
- Gathering information from trustworthy sources
- Analyzing evidence
- Surveillance
- Going undercover
- Analyzing the financial statements

**Notes:** Reviewing public documents and performing background checks

Public documents include any information in the public database, corporate records, or any information on the internet. These public documents are scrutinized as it is straightforward to obtain them. Also, through a thorough background check of a particular company, the business's past dealings are identified under forensic accounting.

**Conducting interviews**

Conducting an interview is an important method that can transform an unwilling person into a source of valuable information. It helps in understanding the facts altogether. It shall be conducted by appropriately assessing the situation's gravity and preparing the questions according to it. The discussions need every detail into account and look at a bigger picture to determine the magnitude of the illegal activity and find the responsible culprit.

**Gathering information from trustworthy sources**

The information gathered by a confidential and trustworthy source is precious. When a piece of information is gained from a confidential source or a confidential informant, all the necessary precautions must be taken to hide the said cause's identity. A forensic accountant must attempt to have as many confidential sources as possible because these types of sources can virtually guarantee a positive result.

**Analyzing evidence**

Making a proper analysis of the collected evidence can point out the guilty party and assist in understanding the extent of fraud committed in the business. This analysis will also help in concluding the company's security against financial scams and installing several measures to prevent such a situation.

**Surveillance**

The surveillance can be done electronically or physically. It is undertaken to uncover any fraud. This can be done by monitoring and tracking all the official emails and messages.

**Going undercover**

This is a severe measure and must only be used as a last option. It is better to leave this issue to the professionals, whoknow how and where to conduct the investigations.

**Analyzing the financial statements**

This is a valuable tool to find out the committed fraud. All the essential details are summarized under the financial statement, and analyzing these statements can help a forensic accountant figure out all the scams.

## 1.9 Development of Forensic Accounting in India

Forensic accounting was not formally defined until the 1940s. Originally Frank Wilson is credited with the birth of Forensic Accounting in the 1930s. When Wilson was working as a CPA for the US Internal Revenue Service, he was assigned to investigate the transactions of the infamous gangster Al Capone. Capone was known for his involvement in illegal activities, including violent crimes.

However, it was Capone's Federal Income Tax fraud that Forensic Accountants discovered. Wilson's diligent analysis of the financial records of Al Capone indicted him for Federal Income tax evasion.Capone owed the government $215,080.48 from illegal gambling profits and was found guilty of tax evasion, for which he was sentenced to 10 years in Federal Prison. This case established the significance of Forensic Accounting.

Maurice Peloubet, a New York CPA, first coined the term "Forensic Accounting" in 1946, and its inspiration came from the responsibility of reconstructing financial enigmas to prove fraud and embezzlement.Maurice E. Peloubet was a leader in the field of accountancy during the first half of the last century who contributed to the profession and, in turn, society at large.

The first recorded history of Forensic Accounting as a specialized field in India is credited to the Mauryans. Reference to the discipline "accounting" that investigates frauds is found in Arthashastra (Science of Material Wealth) written by Kautilya.In Mauryan Times, Kautilya was the first person to mention in his famous book KautilyaArthashastra, the famous forty ways of misappropriation.He is also identified as Chanakya or Vishnugupta.

Forensic accounting was an unheardsubject in the boardrooms till the 2000s; much reliance was placed on the internal auditor to identify corporate malpractices. Over the years, the reliance on internal auditors remained. Still, equal emphasis has been brought on bringing forensic investigators in situations involving a conflict of interest, such as possible collusion with employees.

Big scams viz. Ketan Parekh case, Stamp paper scam,2G spectrum case, Satyam case and housing loan frauds etc., demanded the need for developingforensic accounting services in India. Very few chartered accountant firms had a separate wing for examining fraud.But now, many independent firms have been formed for focused and expert forensic accounting and fraud examination services.However, the big four consultancy firms like Deloitte, KPMG, Price Water House Coopers and Ernst and Young dominate this area.

Uncontrollable factors such as pandemics or financial crimes forced the Indian government, law enforcement agencies, and the industry to relook at the country's corporate fraud and compliance landscape.It was also the time that saw the rise in demand fora forensic accountant or forensic investigators.Recognizing these vulnerabilities, the government introduced multiple provisions in the Companies Act, 2013, to help combat fraud and brought the onus of these requirements on the management of companies.The Act also brought white-collar crime into the ambit of the Serious Fraud Investigation Office (SFIO). Over the last few years, the agency has been seen to pick up several investigations suo-moto.

### Building a career in Forensic Accounting

Forensic Accounting is a mix of accounting practice, investigation, and auditing. Hence, these Financial Detectives start mostly (not always!) as traditional Public Accountants/ Chartered Accountants, and then they move on to more specialized departments in Forensic Accounting.

Ideally, accounting professionals, such as CA/CPA, are preferred for being hired in the investigations team. Someone having a credential, such as a Certified Fraud Examiner (CFE) from the Association of Certified Fraud Examiners (ACFE), is preferred.The Forensic Accounting team is usually a mix of – CPAs, CA's, MBA's, Engineers, CS, Lawyers, Graduates and much more.Many of them do various certification courses to specialize in Forensic Accounting.

Thus,many Forensic Accountants havevarious certifications/qualifications; most importantly, they have relevant experience in Forensic Accounting.

## 1.10 Forensic Accountant: Meaning and Role

Forensic Accountants are experts who use their accounting knowledge with investigative skills and apply this unique combination in investigative accounting settings and litigation support. Forensic Accountants are hired by public accounting firms, risk consulting firms, lawyers, law enforcement agencies, government organizations, insurance companies, or financial institutions. Due to society's increased awareness and growing intolerance of fraudulent activity, the demand for forensic accountants is increasing rapidly.

### Role of Forensic Accountant

A forensic accountant is often retained to analyze, interpret, summarize and present complex financial and business information that is understandable and adequately supported.A Forensic Accountant is often involved in the following:

- Investigating and analyzing financial evidence;
- Developing computerized applications to assist in the analysis and presentation of financial evidence;
- Communicating their findings in the form of reports, exhibits and collections of documents; and
- Assisting in legal proceedings, including testifying in court as an expert witness and preparing visual aids to support trial evidence.
- To properly perform these services, a Forensic Accountant must be familiar with legal concepts and procedures. In addition, a Forensic Accountant must be able to identify substance over form when dealing with an issue.

A forensic accountant can be hired to perform either one or more of the following functions:

- Advice
- Identification of key documents
- Preparation of report
- Review of reports
- Briefing
- Initiative in Environmental Accounting
- Suggestions
- Criminal investigation
- Occupational frauds
- Fraud risk assessment
- Due Diligence
- Information security risk assessment
- Asset tracing
- Vendor monitoring
- Litigation support

*Notes*

### Advice

Giving preliminary advice as an initial appraisal of the pleading and evidence available at the start of proceedings.

### Identification of key documents

Identifying the essential documents which should be made available as evidence. This is important when the forensic accountant is acting for the defence and lawyers are preparing lists of documents to tender in court.

### Preparation of report

Preparing a detailed report on the quantum of evidence, written in a language readily understood by a non-accountant and dealing with all issues, irrespective of whether or not they are favourable to the client.

### Review of reports

Reviewing the expert accounting reports submitted by the other party may impact the quantum of evidence and advise lawyers on these reports.

### Briefing

Briefing legal counsels of the financial and accounting aspects of the case during pre-trial preparation.

### Initiative in Environmental Accounting

Forensic accountants can initiate measuresto introduce environmental accounting to highlight the damage done to the environment by any economic entity. He can prepare a report and make all calculations to assess the possible recoupment of such damages or replenishment of lost properties through environmental management.

### Suggestions

Experience and various types of engagement in financial crimes enable the forensic accountant to offer suggestions for internal control that owners could implement to reduce the likelihood of fraud.

### Criminal investigation

Besides, the forensic accountant will also engage himself in criminal Investigation on behalf of the Police Force or other regulatory bodies, where his report is prepared to present evidence professionally and concisely.

The overall objectives in typical investigations are to:

- Investigate and determine if the alleged material financial irregularities and improprieties have occurred.
- Attempt to quantify whether or not any of these alleged financial irregularities resulted in monetary loss.
- Attempt to identify the persons who could be responsible for the financial irregularities and improprieties.
- These services are required by banks, corporates, and regulators such as RBI, SEBI and law enforcement details.

These assumptions often involve a detailed analysis of numerous years' accounting records to qualify the issues in dispute. He does need an understanding of legal issues of business activities.

### Occupational fraud

The occupational fraud committed by employees usually involves the theft of Assets and embezzlement and the involvement of employees in kickback schemes or conversion of corporate assets for personnel use. The forensic accountant can intervene and observe the suspected examination of assets, invigilation, inspection or documents and interview those involved to control such practices.

### Fraud risk assessment

Managing the risk of fraud is a crucial and integral part. The upcoming Basel -II Accord and the Sarbanes Oxley Act are the by-products of fraud risk. A fraud risk assessment creates an environment that frustrates the fraudster.Interaction of clients with the Fraud Risk experts helps leverage the knowledge of the cultural and working environment dynamics. This approach allows for an immediate buy-In on the recommendations made, as the client has been a part of the risk assessment exercise.

### Due Diligence

It enables the clients to enter a foreign market or open a foreign operation; seek new sources of capital; recruit new dealers, franchisees; or distributors; license their product or service to another company; establish a joint venture or a strategic alliance, acquire or merge with another business; extend credit; appoint directors etc. These kinds of investigations can also be carried out with the help of forensic accountants.

### Information Security Risk Assessment

It includes formulating policies, practices and procedures to prevent any sensitive and confidential information loss. These services address clients' concerns regarding safeguarding critical information against unethical and illegal attempts by rivals and interested parties.Forensic accountants with technology exposures are the best candidates for the information security risk assessment role. The USA Sarbanes Oxley act has compelled these companies to assess their

information security systems. Generally, software companies prefer the technology forensic accountants for the same.

### Asset Tracing

The stamp paper scam was the biggest scandal amounting to over 30,000 crores of rupees. However, when Abdul Karim Telgi was arrested, he had assets worth a few billion rupees.Understanding bank transfers is a technical job that has to be looked at with suspicion. The involvement of Benami Transactions in creating assets makes it even more difficult for law officials to recover the assets.Tracing and identifying client assets that are in the unlawful possession or control of third parties is the area that is looked after by forensic accountants worldwide.

### Vendor Monitoring

Companies involved in the production and marketing of consumer products internationally have become increasingly aware of the importance of monitoring their vendors' labour and business practices.Similarly, the bankers also track their borrowers. For such monitoring services, forensic accountants are preferred by organizations.

### Litigation support

The renowned forensic accountants provide opinions on technical questions of audit, taxation or other areas. It may also involve quantifying losses in the context of fraud, disputed business valuations, loss of profits, insurance claims, intellectual property disputes, and many other situations.

## 1.11 Forensic Accountant: Characteristics and Qualities

The following are the essential qualities a forensic accountant should possess:

- Ethical
- Analytical or problem solver
- Detail-Oriented
- Inquisitive
- Intuitive
- Persistent
- Insightful
- Sceptical
- Confidence
- Others

*Notes*

### Ethical/ Integrity

A forensic accountant should conduct his investigations with utmost integrity, which is a crucial element of character fundamental to the accounting profession. When your primary task is rooting out those, who have committed crimes, you need a strict code of morals and ethics.

This is one area where youwill probably be unable to fake it for very long. And if you develop a reputation as an investigator that cannot be trusted to do the right thing, you won't be investigating anything.

### Analytical or Problem solver

Forensic accountants need to be analytical. As they review financial reports and source documents, they need to analyze the validity of each transaction and determine if the company recorded the transaction fairly.

Sometimes, the documentation will not support the numbers on the reports. The forensic accountant needs to analyze where the numbers on the reports came from and whether the company accurately reported those numbers.

Essentially, being analytical means you are good at breaking down problems into smaller parts to find a solution. It should be no surprise to find this characteristic strongly associated with this career.To be analytical requires focus and brainpower. Problems posed to you while working in this field are likely large and complicated because people try to hide their crimes amidst the sheer volume of information.

### Detail-Oriented

A forensic accountant needs to be detail-oriented. Reviewing financial reports and supporting documents requires looking at large quantities of numbers. At each step, the numbers from the supporting documents need to match the numbers on the financial reports. The forensic accountant needs to compare these amounts and note any inconsistencies.

This requires seeking detailed information for each transaction and investing time to compare the details with the final totals. A good forensic accountant probably needs to have some inherent bent towards detailed information.

*Caution*

As opposed to analytical thinking, it is harder to learn how to be detail-oriented; at its essence, this means he needs to be able to see beneath the apparent effects to uncover the causes.

A detail-oriented person is efficient, hyper-organized, and not willing to accept anything less than a perfect result. As you might imagine, due to the volume of information often presented, this career would not be suitable for someone who is unorganized or makes no use of systems to ensure essential pieces of information donot slip through the cracks.

### Inquisitive

Gaining the information necessary to investigate financial reports comes from asking questions. Inquisitive forensic accountants get answers. As the forensic accountant reviews the numbers on the financial reports, he must ask the staff questions regarding each reported number.

The more questions he asks, the better he will understand why they reported the numbers that appear on the financial reports. If the staff members fail to answer his questions, he needs to continue asking other staff members or supervisors.

### Intuitive

Intuition is the ability to make logical leaps without conscious reasoning, taking in disparate pieces of information and automatically making connections. This isnot to say an unintuitive person cannot work as a financial investigator, but he or she might find the going more challenging.

### Persistent

Persistence plays avital role in the life of the forensic accountant. In some cases, the financial reports lack supporting documentation. The forensic accountant must continue requesting that documentation and finding the reported data source.

Without the supporting documentation, the forensic accountant cannot conclude the validity of the numbers. He needs to continue requesting the documentation and becoming more assertive until he can make a solid conclusion.

### Insightful

Being able to pick up on critical details and make intelligent observations that may otherwise go overlooked is a prerequisite in investigative accounting.

### Sceptical

The role of the investigative accountant personifies the sceptical attitude, one that refuses to take anything at face value.

### Confidence

The daily duties of the forensic accountant involve prying exceptionally profoundly into the financial activities and general dealings of others. Their presence is not always appreciated as the outcome of their efforts could have severe legal repercussions. This, in turn, calls for an individual of unshakable confidence and conviction.

Thus, a forensic accountant must focus on his work even though many present persons do not like his presence.

**Others**

Other qualities include responsiveness, being evaluative, patience, tech-savvy, functioning well under pressure, being a team player, being adaptive, making people feel at ease and being able to generate new ideas.

## 1.12 Forensic Accountant: Skills

Theskills required by an individual to function well as a forensic accountant can be categorized into two:

a) Core Skills
b) Enhanced Skills
   a. Core Skills: These are the following skills that are foundational to the forensic accountant.
      - Critical/Strategic thinking
      - Identify key issues
      - Auditing skills
      - Effective oral communicator
      - Effective written communication
      - Simplify information
      - Positive criminal mind
      - Eye of details
      - Investigative ability
   b. Enhanced Skills: Beyond the core skills identified above, forensic accountants, being specialists and professionals at what they do, also require the following enhanced skills to function optimally at what they do:
      - Analyzing and interpreting financial statements and information
      - Testifying
      - Knowledge of relevant professional standards
      - Audit evidence
      - Fraud detection
      - Asset tracing
      - Electronic discovery/Use of Technology
      - General knowledge of rules of evidence and civil procedure
      - Interviewing skills
      - Possess specialized technical skills
      - Internal controls
      - Conflict negotiation and resolution
      - Knowledge of law enforcement

*Notes*

Critical/Strategic thinking:A forensic accountant should be able to constantly think critically, see issues beyond the surface, and make logical connections between ideas to make a sound judgement.

Identify critical issues**:**A forensic accountant should always be able to identify key points in the volume of information being processed.

Auditing Skills**:**Aforensic accountant must understand the audit principles well andbe able to do an audit by applying those principles. Auditing, in many ways, provides a foundation upon which forensic accounting and investigation can build.

Effective oral communicator**:**As a forensic accountant, you must communicate verbally in person and over the telephone. Explaining complex financial issues in simple, layman's terms and answering questions is also essential.

Some accounting jobs require presentations in front of people, such as the board of directors, legal and financial regulators or professional membership organizations. Effective oral communication skills include having the ability to teach in the courtroom.

*Example*

The forensic accountant must have a knack for taking very complex financial data and explaining it to those listening- judge or jury, in a manner they easily understand. If the testifying forensic accountant notices a jury member or two starting to doze off while speaking, this may not be a good sign that they are getting their message across.

Effective written communication**:**In addition to being able to communicate effectively, a forensic accountant must be able to communicate well through writing. This is more so because the work of forensic accountants will almost always end up in a report submitted to the relevant party.

Positive criminal mind (Think like the wrongdoer): There is no doubt that criminals are among the most intelligent people on earth. A successful criminal must be competent to enable him to succeed. A Forensic accountant should be able to think like a criminal; the only difference is that your smartness and street wise-ness should be used in combating crime and not to perpetrate fraud.

Eye for details (See the big picture)**:**A forensic accountant should be someone that hasa knack (talent) for more information. They should see the bigger picture embedded within what many call trivial (of little importance).

Investigative ability**:**Forensic accountants should be able to investigate any matter that comes to their attention appropriately.

Otherskillsinclude research skills, solving unstructured/structured problems, understanding the goals of a case, and synthesizing the results of discovery and analysis.

## 1.13 Forensic Audit: Meaning and Definition

A forensic audit is generally referred to as an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court. It represents an area of finance that combines detective skills and financial acuity. It is an examination and evaluation of a firm's or individual's financial information for use as evidence in court. A Forensic Audit can be conducted to prosecute a party for fraud, embezzlement or other financial claims. In addition, an audit may be performed to determine negligence or how much spousal or child support an individual will have to pay.

**Forensic Audit: Definition**

It is the application of financial skills and an investigative mentality to unresolved issues conducted within the context of the rules of evidence. As a discipline, it encompasses financial expertise, fraud knowledge, and strong knowledge and understanding of business reality and the working of the legal system.

- Jack Bologna and Robert

## 1.14 Forensic Audit: Importance

The importance of Forensic Audit could be rationalized as below:

- Forensic auditing, described as a specialized field of accountancy, investigates fraud and analyses financial information for legal proceedings.
- In a forensic audit, a systematic and independent examination of an organization's books, accounts, statutory records, documents and vouchers is held to ascertain fraud or probability of fraud.

- Much beyond the official documents of the company, the Forensic audit involves a lot of fieldwork, trying to talk to multiple stakeholders to gather information and then look for evidence to corroborate it.
- It also attempts to identify or corroborate the culprit behind the fraud.
- It arranges and collects the evidence of the fraud and the person accused of fraud.
- The collected evidence and reviewed facts are used in the legal proceedings, which assist the court in granting punishment to the real accused of the fraud.
- Forensic auditing uses accounting, auditing, and investigative skills to investigate theft and fraud. It encompasses both Litigation Support and Investigative Accounting.

This makes forensic audit an apt tool in contemporary times, ensuring the financial health of the companies through aiding in the Prevention, Regulation and Penalization of financial frauds and scams.

## 1.15 Forensic Auditor: Meaning and role

A Forensic auditor is often retained to analyze, interpret, summarize and present complex financial and business-related issues in an understandable and adequately supported manner. Forensic Auditors can be engaged in public practice or employed by insurance companies, banks, police forces, government agencies and other organizations.

The Role of a Forensic Auditor may be understood as follows:

- Criminal Investigations
- Personal Injury Claims
- Fraud Investigations
- Investigation and Inspection
- Expert Opinion
- Professional Negligence
- Expert Witness Cases
- Meditation and Arbitration
- Litigation Consultancy
- Computer Forensics
- Evidence
- Report
- Court

*Notes*

### Criminal Investigations

Forensic auditors would use their investigative accounting skills to examine the documentary and other available evidence to give their expert opinion on the matter. Their services could also be required by Government departments, the Revenue Commissioners, etc. for investigative purposes. Practising forensic auditors could be called upon by the police to assist them in criminal investigations that could relate to individuals or corporate bodies.

The investigation is carried out, focusing on suspicion of the client. If a client suspects there might be some fraud in his company on the materials supplied, for example. The forensic auditor goes ahead to find out:

- What type of fraud is carried out (if there's any)?
- The time the fraud has been taking place
- How the fraud was concealed, and the people involved in it
- The impact of the fraud on the company

### Personal Injury Claims

Where losses arise due to personal injury, insurance companies sometimes seek expert opinion from forensic auditors before deciding whether the claim is valid and how much to pay.

### Fraud Investigations

A forensic auditor might be called upon to assist in business investigations involving funds tracing, asset identification and recovery, forensic intelligence gathering and due diligence review.In cases involving fraud perpetrated by an employee, the forensic auditors will be required to give their expert opinion about the nature and extent of fraud and the likely individual or group of individuals who have committed the crime.The forensic expert undertakes a detailed review of the available documentary evidence and forms their opinion based on the information extracted during that review.

### Investigation and Inspection

A forensic auditor may help the Police, ACB (Anti-Corruption Bureau) and other investigating authorities collect evidence and other investigation purposes. For example, section 157 of The code of Criminal Procedure, 1973; sections 17 and 18 of the Prevention of Corruption Act, 1988;Section 6 of The Bankers Books Evidence Act, 1891; Section 78 of Information Technology Act, 2000; Section 447 of the Companies Act, 2013 states that the Court or Police may require the skills of Forensic auditors while inspecting any books in so far as related to the accounts of an accused.

### Expert Opinion

Forensic auditors carefully examine the accounts and balance sheets. They use their skills to determine whether fraud is committed or any anomaly associated with it by givingtheir expert opinion.

### Professional Negligence

The forensic auditor might be approached in a professional negligence matter to investigate whether professional negligence has taken place and to quantify the loss resulting from the negligence.

### Expert Witness Cases

The forensic auditor often attends court to testify as an expert witness in civil and criminal court hearings. In such cases, they present investigative evidence to the court to assist the presiding judge in deciding the outcome of the case.

### Meditation and Arbitration

Some forensic auditors, because of the specialist training they would have received in legal mediation and arbitration, have extended their forensic auditing practices to include providing Alternative Dispute Resolution (ADR) services, in the absence of which a matter could be expensive and time-consuming for individuals or businesses involved in commercial disputes with a third party.

### Litigation Consultancy

Forensic auditors are eligible to be engaged in litigation and assist with evidence, strategy and case preparation.

### Evidence

This is the critical part of the investigation since it is the main reason for the auditing to be carried out. The forensic auditor is expected at the end of the audit to present full evidence showing the type of fraud that was carried out, and the effect of the fraud to the company and the people involved.

Here are the techniques used to gather evidence.

- Substantive Procedure

This is where the auditor reviews the complete documentation of the company concerning the area of investigation to find out if there are any inaccurate material statementsand the validity of the materials and reviews the accuracy of the financial records.

- Analytical Procedure

This helps the auditor to understand the client's business and changes in the industry. He uses this to compare the different periods of time on the company's expenditure/budget, for example.

- Software Programs

Forensic auditors have their own software programs that can detect any fraud that might have been carried out using technological devices like computers.

- Internal Controls

The forensic auditor takes time to understand and test the internal control system to find out if there are any holes in the system that would have allowed the fraud to occur.

**Report**

At the end of the audit, the auditor reports the fraud to the client.The report should include:

- Findings of the report
- Evidence summary
- Information on how the fraud was carried out
- Recommendations on how the fraud can be avoided from occurring in the future
- The report is the one that the client uses as evidence in court if he decides to file a case.

**Court**

During the court proceeding, the auditor must be present to explain how he collected the evidence and identified the suspect(s).

The auditor should explain all the processes using simple terms (this is for people who don't understand the accounting terms).

That being said, it is true that a forensic auditor plays a considerable role, but he does not work alone. To hire a forensic auditor, you must decide which forensic accounting firm to contact.

## 1.16 Forensic Auditors: Qualities

A forensic auditor should have the following qualities to fulfil his professional role effectively:

- Expert in Accounting and Auditing
- Must have in-depth knowledge of the business regulatory environment
- Problem-Solving skills
- Tech-Savvy
- Patience
- Ethical
- Investigative mind
- Intuitive
- Confident
- Inquisitive
- Persistent
- Effective communication skills

## 1.17 Forensic Audit Vs. Financial Audit

Financial auditing aims to express an opinion about'true & fair' presentation. A forensic Audit determines the correctness of the accounts or whether any fraud has occurred.

Techniques used in financial auditing are more 'Substantive' and 'compliance' procedures. The methods used in forensic auditing are analysis of past trends and substantive or 'in-depth' checking of selected transactions.

Typically all transactions for a particular accounting period are covered under financial audits. Forensic audits donot face any such limitations. Forensic auditors may be appointed to examine the accounts from the beginning.

For ascertaining the accuracy of the current assets and liabilities, the financial auditor relies on the management certificate or representation of management. Forensic auditors are required to carry out the independent verification of suspected or selected items.

## 1.18 Forensic Accounting Vs. Forensic Auditing

Severalpersons use forensic accounting and forensic audit as synonyms. But these terms are significantly different.Both professions deal with financial evidence but differ in methods, techniques and tools used in the process.

The maindifference between forensic accounting and auditing lies in the purpose of the audit. A forensic accounting assignment related to fraud against the business. This issue may involve employee fraud or a dispute with a vendor or customer.

However, forensic auditing is related to fraud for the business. Forensic audits relate directly to financial statement fraud, whereas forensic accounting requires investigative techniques and technology.

Forensic Accounting assignments are complex. Do forensic accountants enquire about who perpetrated the fraud? What was the modus operandi? And what were the fraud losses for an organization?

On the other hand, forensic auditors check the money trail. Source of funds to utilization, forensic auditors answer the questions such as the motives of the business behind the fraud.

Forensic auditors witnessed a boom in India when bankers started scouting for experts to ascertain willful default in borrower accounts.In the proceedings of NCLT or asset reconstruction mechanism, forensic audits play a crucial role. Law enforcement agencies often summon forensic auditors to investigate Ponzi schemes.

Forensic Accountants need different analytical tools based on the scenario they investigate. Many times the scope of forensic accounting is challenging. Forensic Accountants look beyond numbers; they use digital forensic tools to recover the deleted data and CDR tools to analyze mobile phone records. They use expert witnesses to unearth signature forgery. Government Agencies such as revenue departments may summon forensic accountants to take the image of the computer system to recover the deleted data and to analyze the emails, which can be produced in a court to recover the taxes

Forensic Audits primarily deal with the trail of money. But the work becomes challenging when the expert Public Accountants or advisors create layers of entities to route the transactions.

Court cases requiring the evidence provided by a forensic accountant may include commercial litigation, business valuation, divorce, bankruptcy and, of course, fraud.Forensic audits require analysis of financial transactions and compilation of the information for use in court cases. The forensic auditor may also examine a company's financial records to determine reliability, accuracy and the strength of internal controls systems.

## 1.19 Who appoints Forensic experts

Financial audits confirm information such as bank balances or vendor and customer accounts with the appropriate third parties. This provides the necessary confirmation of the company's accounting practices and standards. Many of the procedures followed in forensic audits are similar to regular audits. The regulators order forensic Audits, revenue authorities or bankers to probe business matters and verify accounting records.

On the other hand, forensic accountants are appointed by the business when they suspect fraud or data leakage. Such an assignment aims to identify the evidence produced in the court of law. In India, very few accounting firms deal in this aspect. Forensic Audit firms are relatively large in numbers due to the regulatory requirements. Enforcement of the Insolvency act created new avenues for forensic auditors.

Both forensic experts closely examine and confirm financial position using different methods. Both assignments differ significantly in their end product. As companies engage forensic accountants to

answer specific questions, a standard forensic accounting report format does not exist. However, the forensic auditor must provide the requested information and supply sufficient evidence to argue the results in court.

## Summary

- The investigation of fraud or financial irregularities by performing extremely detailed research and business information analysis is forensic accounting.
- It is sometimes called investigative accounting,which combines accounting and auditing with information technology.
- 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.
- It is a widely applied accounting discipline that resolves financial conspiracies—money laundering, bankruptcy, embezzlement, insurance claims, securities fraud, asset misappropriation, tax evasion, divorces, family disputes, financial frauds, and debt defaults.
- A single person cannot execute forensic processes. Instead, it is carried out by a structured team of professionals and experts like Certified Public Accountants (CPAs), Chartered Accountants (CAs, Forensic Accountants, Management and Cost Accountants, Auditors etc.
- A forensic accountant is often retained to analyze, interpret, summarize and present complex financial and business information that is understandable and adequately supported.
- A forensic audit is generally referred to as an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court.
- Forensic Auditing is used in several ways for many purposes, not just for criminal activity detection.
- Forensic audits are becoming increasingly frequent for top leadership searches as stringent corporate governance norms, and increasing stakes are prompting Indian and multinational companies to ensure that the people they take on board have no flaws on their track record.

## Keywords

Audit: Audit means an official inspection of an organization's accounts, typically by an independent body.

Forensic accountant: Forensic Accountants are experts who use their accounting knowledge with investigative skills and apply this unique combination in investigative accounting settings and litigation support.

Forensic accounting combines accounting, auditing and investigative skills or techniques to discover financial crimes and assist in legal matters or proceedings.

Forensic audit: It represents an area of finance that combines detective skills and financial acuity.

Fraud: It generally refers to a wrongful or criminal deception practised which is intended to result in financial or personal gain to oneself and a financial or personal loss to the other.

Lawsuit: It is a specific legal action wherein the plaintiff files a complaint with the court.

Litigation: It is the process used to resolve a lawsuit.

## SelfAssessment

1. The investigation of fraud or financial irregularities by performing extremely detailed research and business information analysis is _____.

A. Accounting
B. Financial Accounting
C. Forensic Accounting
D. Forensic Auditing

2. _____ is a type of white-collar crime that involves taking the cash of a business before entering it into the accounting system.

A. Insurance fraud
B. Money laundering
C. Skimming fraud
D. Securities fraud

3. Ponzi schemes are an example of:

A. Business fraud
B. Asset Misappropriation
C. Skimming fraud
D. Securities fraud

4. Forensic experts quantify _____ in vehicular accidents.

A. Economic damages
B. Employee lost wages
C. Cash embezzlement
D. Business claims

5. The following is the specialized forensic knowledge as per AICPA:

A. Laws, Courts, and Dispute Resolution
B. Planning and Preparation
C. Information Gathering and Preserving
D. Financial Statement Misrepresentation

6. The following forensic accounting reports can be prepared to support the different litigations in court:

A. Earnings report
B. Death report
C. Patent violation report
D. All of above

7. The following report focuses on determining the subsequent loss of wrongful dismissal of an employee.

A. Income statement of the company

B. Earnings report
C. Dismiss report
D. Death report

8. A _____ could also be the expert witness testimony on how the Fraud is committed in the court.
A. Company Secretary
B. Company Auditor
C. Company Lawyer
D. Forensic Accountant

9. Who is not responsible for investigating and quantifying the fraud that happens in the company?
A. Auditor
B. Forensic Auditor
C. Forensic Accountant
D. Forensic Expert

10. The litigation process cannot continue after a lawsuit is resolved.
A. True
B. False

11. Forensic accounting is generally described as accounting that is used for:
A. Interview purposes
B. Legal purposes
C. Investigative purposes
D. Charting purposes

12. The scope of forensic accounting is restricted to Bank Forensic Audits.
A. True
B. False

13. _____ is an important method that can transform an unwilling person into a source of valuable information for a forensic accountant.
A. Public documents and background checks
B. Interviews
C. Financial statements
D. Surveillance

14. Annual reports are generally available on each public company's website. Financial statements presented in the annual reports are an example of:
A. Public document
B. Hidden evidence

C. Private document
D. Background check evidence

15. A forensic accountant can perform surveillance to uncover fraud.
A. Electronically
B. Physically
C. Both Electronically and Physically
D. Either Electronically or Physically

16. Who is credited with the birth of Forensic Accounting in the 1930s?
A. Frank Wilson
B. Al Capone
C. AICPA
D. Mauryans

17. Who is the author of Arthashastra (Science of Material Wealth)?
A. Kautilya
B. Mauryans
C. Maurice Peloubet
D. Frank Wilson

18. What forced the Indian government, law enforcement agencies, and the industry to relook at the country's corporate fraud and compliance landscape?
A. Increasing incidents of Financial collaborations
B. International bodies
C. Forensic accountants
D. Rapid increase in Financial crimes

19. Only Chartered Accountants (Cas) can pursue the profession of Forensic Accountants.
A. True
B. False

20. The Forensic Accounting team usually has:
A. A mix of CAs, CPAs and Lawyers
B. MBAs and Lawyers
C. MBAs and Engineers
D. A blend of CAs, CPAs, MBAs, Engineers and Lawyers

21. When forensic accountants provide opinions on technical questions of audit, taxation or other areas. Their ideas come under the purview of:
A. Vendor monitoring
B. Litigation support
C. Due diligence

D. Information security risk assessment

22. "The more questions he asks, the better he will understand" belongs to which of the following qualities of a forensic accountant?

A. Analytical or problem solver

B. Detail-Oriented

C. Inquisitive

D. Intuitive

23. A forensic accountant should conduct his investigations with the utmost integrity. Thus, he should be _____ person.

A. Ethical

B. Inquisitive

C. Intuitive

D. Sceptical

24. Select the enhanced skill of a forensic accountant from the following list of skills.

A. Simplify information

B. Positive criminal mind

C. Eye of details

D. Testifying

25. "Conflict negotiation and resolution" is _____ skill of a forensic accountant.

A. Enhanced

B. Core

C. Fundamental

D. Both enhanced and core

26. The services of forensic auditors could be required by:

A. Government departments

B. Both Government departments and Regulatory bodies

C. Both Regulatory bodies and Revenue Commissioners

D. Government departments, Regulatory bodies and Revenue Commissioners

27. A forensic auditor is not required to be Tech-Savvy.

A. True

B. False

28. _____ is related to frauds for the business.

A. Forensic Sciences

B. Forensic Auditing

C. Forensic Accounting

D. Financial Auditing

29. _____ are appointed by the business themselves when they suspect a fraud or data leakage.

A. Forensic Auditors
B. Auditors
C. Accountants
D. Forensic Accountants

30. A forensic auditor can be indulged in criminal investigations projects.

A. Yes
B. No
C. May be
D. Can't say

## Answers for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | C | 2. | C | 3. | D | 4. | A | 5. | D |
| 6. | D | 7. | B | 8. | D | 9. | A | 10. | B |
| 11. | B | 12. | B | 13. | B | 14. | A | 15. | C |
| 16. | A | 17. | A | 18. | D | 19. | B | 20. | D |
| 21. | B | 22. | C | 23. | A | 24. | D | 25. | A |
| 26. | D | 27. | B | 28. | B | 29. | D | 30 | A |

## Review Questions

1. Define forensic accounting. Write key characteristics of forensic accounting.
2. Write types of forensic accounting.
3. Discuss the applications of forensic accounting as per AICPA.
4. Explain the role of forensic accounting in litigation support and criminal investigation.
5. Discuss the scope and importance of forensic accounting.
6. Write a note explaining the meaning of a forensic accountant.
7. Explain the role of a forensic accountant.
8. Explain the qualitative characteristics of a forensic accountant.
9. Does a forensic accountant need specific skills to perform their role effectively? If yes, which skills must they have? Explain.
10. Write a short note on forensic audit. Discuss the importance of forensic audit.
11. Explain the various reasons for hiring a forensic auditor's services.
12. Summarize the role of a forensic auditor.
13. List the qualities of an effective forensic auditor.
14. Which qualifications are required to be a forensic expert?
15. What do you mean by forensic audit? Discuss its need and significance in detail.

16. Write down the similarities and differences between Financial Audit and Forensic Audit.
17. Compare Forensic Accounting with Forensic Auditing.

## Further Readings


- Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). *Forensic Accounting and Fraud Investigation* (CPE ed.). John Wiley & Sons.


### Web Links

- https://www.wikiaccounting.com/what-is-forensic-accounting
- https://enterslice.com/forensic-accounting-and-investigation
- https://www.accaglobal.com/an/en/student/exam-support-resources/professional-exams-study-resources/p7/technical-articles/forensic-accounting.html
- https://www.affluentcpa.com/role-forensic-auditor/
- https://indiaforensic.com/career-path-of-forensic-accountant/
- https://indiaforensic.com/every-chartered-accountant-can-not-be-a-forensic-auditor/
- https://indiaforensic.com/forensic-audit-profession-in-india/
- https://www.affluentcpa.com/role-forensic-auditor/

# Unit 02: Fraud Taxonomy

CONTENTS



## Objectives

After studying this unit, you will be able to:

- Explain the meaning and elements of fraud.
- Illustrate the fraud triangle.
- Explain the types of fraud.
- Review the reasons of committing fraud.
- Comment on the psychology of fraudster at times of committing fraud.

## Introduction

Fraud is an intentional deception of a material fact and includes lying, stealing and cheating. it consists of coercing people to act against their own best interest. The intentional act means to induce another person to part with something of value or to surrender a legal right. Fraud can range from a minor theft by an employee to a large scale misappropriation of assets or manipulation of financial statements. The loss from fraud far exceeds the loss from robbery.

Punjab National Bank (PNB) scam is a recent example of a business entity whose employees misrepresented the facts and committed fraud for Nirav Modi. Enron is an another example of a corporate whose management misrepresented the company's financial position and committed fraud. Financial statement fraud, employee fraud like the Enron fraud and PNB fraud, are just few of the many types of frauds that represent major problems for businesses throughout the world.In broadest sense, fraud is a deception made for personal gain.

## 2.1 Meaning and Types of Fraud

### Meaning of Fraud

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. Fraud is a broad category of financial-related crimes and includes confidence schemes, art forgery, falsified scientific research data, lying on a resume,

falsifying an insurance claim, cheating on income taxes, and hundreds of other possible schemes that would fall under the term "fraud."

White-collar crime should be viewed as a subclass of fraud. Individuals commit white-collar crime by embezzling funds, manipulating accounts, receiving bribes, or committing other schemes through their place of business. What they all have in common, however, is the intent to deceive.

As defined in Section 17 of the Indian Contract Act, 1872,

"Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent , with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:—

(1) Thesuggestion, as a fact, of that which is not true, by one who does not believe it to be true;

(2) Theactive concealment of a fact by one having knowledge or belief of the fact;

(3) Apromise made without any intention of performing it;

(4) Any other act fitted to deceive;

(5) Anysuch act or omission as the law specially declares to be fraudulent.

**Caution:**Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak , or unless his silence is, in itself, equivalent to speech.

As per Section 447 of the Companies Act, 2013,

"Fraud", in relation to affairs of a company or anybody-corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

Black's Law Dictionary defines fraud as a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. It could be a tort (civil matter) or it could be criminal.

Thus, it is inferred that fraud can also be a civil wrong (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal wrong (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities) or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong.

## Elements of Fraud

Fraud is deception that includes the following elements:

- **False and Wilful representation or assertion**: In the absence of representation or assertion except in the following two cases, there can be no fraud.
- Where silence may itself amount to fraud, and
- Where there is active concealment of facts

**Example**: Cheetah, intending to deceive Tiger, informs him that his estate is free from encumbrance. Tiger thereupon buys the estate. The estate is, however, subject to mortgage. The contract is induced by fraud.

- **Perpetrator of Representation**:The false representation or misstatement must have been made by a party to the contract or by anyone with its connivance, or by its agent. If a stranger makes the misstatement to the contract, it cannot result in fraud.

**Example**: Aurella suggests Bruno to buy Droopy's car, which according to Aurella runs 15 kms per litre. Later on, Bruno finds that the car runs only 8 kms per litre. Aurella was, however, acting neither at the instance of Droopy nor was his agent; he was a stranger. The

contract that took place between Bruno and Droopy cannot be stated to be induced by fraud.

- **Intention to deceive:**Intention to deceive the other party is the essence of fraud. In order to commit a fraud, one person asserts or misstates the fact with the intention that it should be acted upon.

**Example**: Ankush, intending to deceive Bhanu, falsely represents that 1,000 tons of sugar is produced annually at his factory, although Ankush is fully aware that only 600 tons of sugar can be produced annually. Bhanu thereby agrees to buy the factory. Ankush has resorted to fraud to obtain the consent of Bhanu.

- **Representation must relate to a fact**: The representation made by the party must relate to a fact, which is material to the formation of the contract. A mere statement of opinion, belief, or commendation cannot be treated as fraud.

**Example:** Anuj states that the detergent produced at his factory washes whiter than whitest. The statement made by Anuj is merely a commendation of the product and not a fact. Thus, it does not amount to fraud.

- **Active concealment of facts:**Active concealment implies 'when the party takes positive or deliberate steps to prevent information from reaching the other party and this is treated as fraud.'

**Example:** Ammi sells a horse to Boomer in an auction despite knowing that the horse is unsound. Ammi says nothing to Boomer about the horse's soundness. This is a case of passive concealment of fact and cannot tantamount to fraud.

**Did you know?**

What is passive concealment?

Passive concealment implies mere silence as to material facts, which barring a few cases, does not amount to fraud.

- **Promise made without intention of performing it**: If a person while entering into a contract has no intention to perform his/her promise, there is a fraud on his/her part, for the intention to deceive the other party is there from the very beginning.
- **Representation must have actually deceived the other party**: The representation made with the intention to deceive must actually deceive. The party, induced by fraudulent statement, must have relied on it to accord its consent.
- **Any other act fitted to deceive:**The expression 'any other act fitted to deceive' obviously means any act, which is done with the intention of committing fraud. This category includes all tricks, dissembling, and other unfair ways, which are used by cunning and clever people to cheat others.
- **Any such Act or omission that the law specially declares as void:**This category includes the act or omission that the law specially declares to be fraudulent.
- **Wrongful Loss and Wrongful Gain is Immaterial.**For the purposes of "Fraud" under the Companies Act, 2013, it is immaterial whether there has been some wrongful loss to one and/or wrong gain to another. The only important thing is intention to deceive and the act or omission actually deceiving the victim. Common corporate frauds for example are, if the CMD husband benefits from a loan transaction sanctioned by her it is a fraud. If a CEO take bribe to approve a contract that is a fraud.

On the same principle, Indian Penal Code too works, as for IPC to constitute an offence, two elements are required which are Mens Rea – Intention to Commit Offence and Actus Reus – The Wrongful Act.

## Types of Fraud

There are many ways to classify fraud. Let's discuss classification of frauds as per few common parameters as below:

### 1. Frauds against or for organization?

a) Frauds against organizations

In employee fraud, fraud is committed against an organization and the victim of the fraud is the employee's organization.

**Example**:PNB scam where some of the PNB employees frauded to help Nirav Modi at the expense of their organization i.e. PNB.

b) Frauds for or on behalf of organizations

In financial statement fraud, executives usually commit fraud "on behalf" of an organization, usually to make it's reported financial results look better than they actually were. In this case, the executives of a company usually benefit because a company's stock price increases or remains artificially high and the victims are investors in the company's stock.

**Example**:Satyam Scam: The founder and directors of India-based outsourcing company Satyam Computer Services, falsified the accounts, inflated the share price, and stole large sums from the company.

### 2. Frauds as per Occupation (Occupational fraud)

Another way to classify frauds is to use the Association of Certified Fraud Examiners (ACFE) definition of "occupational fraud." The ACFE includes three major categories of occupational fraud:

(a) Asset misappropriations, which involve the theft or misuse of an organization's assets,

(b) corruption, in which fraudsters wrongfully use their influence in a business transaction in order to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another, and

(c) Fraudulent statements, which generally involve falsification of an organization's financial statements.

### 3. Frauds as per Victims

(a) Frauds where a company or organization is the victim.

i. Employee embezzlement-perpetrator is a company or an organization employee.

ii. Vendor fraud-perpetrator is a vendor of the company or an organization.

iii. Customer fraud-perpetrator is a customer of the company or an organization.

(b) Management fraud-victims are shareholders and debt-holders of an organization or a company.

(c) Investment scams and other consumer frauds- victims are unwary individuals.

(d) Miscellaneous frauds-victims could be anyone.

Fraud that doesn't fall into one of the first three types and may have been committed for reasons other than the financial gain is simply labeled miscellaneous fraud. These types of fraud are summarized in the following Table.

**Types of Fraud**

| Types of Fraud | Perpetrator | Victim | Explanation |
|---|---|---|---|
| Employee embezzlement | Employees of an organization | The employer or organization as whole | Employees use their positions to take or divert assets belonging to their employer. This is the most common type of fraud. It can be direct or indirect. |
| Vendor fraud | Vendors of an organization | The organization to which the vendors sell goods or provide services | Vendors either overbill or provide lower quality or fewer goods than agreed. |
| Customer fraud | Customers of an organization | The organization which sells goods to customers | Customers don't pay, pay too little, or get too much from the organization through deception. |
| Management fraud (Financial-statement fraud) | Management of an organization | Shareholders, debt-holders, regulators | Management manipulates the financial statements to make the company look. better than it is. This is the most expensive type of fraud. |
| Investment scams and other consumer fraud | Frauds perpetrators- all kinds | Unwary investors | These types of frauds are committed on the Internet and in person and obtain the confidence of individuals to get them to invest money in worthless schemes. |
| Other (Miscellaneous frauds) | All kinds – depends on the situation | All kinds – depends on the situation | Any time anyone takes advantage of the confidence of another person to deceive him or her. |

Source:Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2009). *Forensic Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.

### 4. Frauds specific to Economy and Financial Transactions

In specific to the impact on economy and financial transactions, frauds could be categorized as below:

1) Bank frauds

2) Corporate frauds

3) Insurance frauds

4) Cyber frauds

5) Securities frauds

1) **Bank Frauds:** Bank fraud is a big problem in today's world. The number of bank frauds in India is substantial. It is in increasing with the passage of time in all the major operational areas in banking. In financial year 2022, the Reserve Bank of India (RBI) reported a total of around 9,103 bank fraud cases across India.

**Examples:**The Rs 34,000-Crore DHFL Scam, ABG Shipyard Scam, The Amtek Auto Case, Bhushan Power and Steel, PNB scam

2) **Corporate Frauds:**In India, Corporate Frauds from leading Indian business are shaking the economy time and again from Satyam Computers which stunned the national financial world in 2009, when Satyam's Founder B. Ramalingan Raju declared he had inflated profit and jacked-up the

company's Balance Sheet by more than one billion dollars to the recent incident of PNB Fraud in year 2017. This needs to be checked strictly to ensure financial stability for emerging Indian economy.

3) **Insurance Frauds:**There is different type of frauds in insurance sectors. E.g. health insurance, claims fraud, false claims, insurance speculations, application frauds etc.

4) **Cyber Frauds:**Cyber Frauds are the frauds done with the help of the internet targeting the unauthorized use of digital instruments like credit card, ATM card, cyber equipment's at home etc.

5) **Securities Frauds**: Apart from Corporate Frauds, Frauds in the Securities Market are also affecting many people time and again. From the perspective of frauds in securities, investor community could not forget the under truncate Rs. 4000 crore of Harshad Metha scam and over Rs. 1000 Crore of Ketan Parekh scams which duped the shareholder with the loss of their wealth in the big markets. In addition to this, the instances of Insider trading are also considered securities fraud in many circumstances. The recent misutilization of clients securities by Karvy for securing loans for sister concern Karvy Reality could also be regarded as a securities fraud.

**Did you know?**

How employee fraud and management fraud differs?

In employee fraud, an individual embezzles from his or her employer, which usually benefits the perpetrator. In management fraud, an organization' officers deceive investors and creditors by manipulating financial statements. It is most often perpetrated to benefit an organization and its officers.

## 2.2 Fraud Taxonomy

There are various terms related to fraud that need to be explained before going into the depth of the concept, types, and consequences of fraud. These terms are introduced below:

### Fraud, Theft, and Embezzlement

The terms fraud, theft, and embezzlement are often used interchangeably since they have some common elements. However, in criminal law, these terms are not identical.

**Fraud**is a criminal deception involving using any false representation to obtain an unjust advantage or injuring the rights or interests of another person.

**Theft**is an intention to take dishonestly any immovable property out of the possession of any person without his/her consent. In other words, theft is referred to as taking away someone else's property, with an intention to deprive the owner of its possession.

**Embezzlement**is dishonest misappropriation of a property by a person who comes in possession thereof lawfully. It is a situation when the perpetrator comes into initial possession of a property lawfully, but then converts it to his/her own use. In embezzlement, the perpetrators have a fiduciary duty to take care now and protect the property but when he converts it to his own use, there is a breach of his fiduciary duty.' Thus, embezzlement is the fraudulent conversion of a property of another by a person who has lawful possession of a property

### Fraud and Human Nature

A man is distinguished from an animal as he has the ability to reason and derive truth, but the same can be used to distort the truth. Truth and justice are idealistic and living concepts that can change from time to time through the experience and discoveries of human beings.

### Skimming and Lapping

Skimming is a 'front-end fraud'. Funds are stolen before a book entry is made. It is a common practice in a cash business, such as bars, restaurants vending machines, home modernization contracting, fuel stations, and retail stores. Lapping is a form of robbery. One takes in customer A's money, steals it, and pays it back the next day with customer B's money. The problem is, that there often is a balloon effect from lapping.

### Fraud as Deception

Fraud can be defined as deception, where deception can be either intentional or unintentional. Deception includes several types of communications or omissions that serve to distort or omit the complete truth. Fraud is an intentional deception of another person through lying and cheating, to derive an unjust personal, social, political, or economic advantage over that other person. Thus, fraud is an intentional deception that includes the following elements:

1. A misrepresentation,

2. About a material fact,

3. Which is false,

4. (And) intentionally,

5. Which is believed,

6. (And) acted upon by the victim,

7. To the victim's damage.

**Caution:**All fraud includes deception, but all deceptions are not a fraud.

### Fraud as a Civil or Criminal Wrong

Civil Law is the body of law that provides remedies for violations of private rights. Civil law deals with rights and duties between individuals. Civil claims begin when one party files a complaint against another, usually to gain financial restitution. The purpose of a civil lawsuit is to compensate for harm done to another individual.

Criminal Law is that branch of law that deals with offences of a public nature. Criminal Laws generally deal with offences against society as a whole.

**Caution:**A civil fraud requires that the victim suffers damages, a criminal fraud requires the proof of an intentional deception.

### Internal and External Fraud

An organization is exposed to the risk of fraud in several ways. While an internal fraud is a fraud that is perpetrated by an individual or individuals inside the organization, external fraud is a fraud that is perpetrated by an individual(s) outside the organization. Internal fraud is also known as an occupational fraud or management fraud. Perpetrators are increasingly embracing technology and new approaches in the commitment and concealment of an occupational fraud.

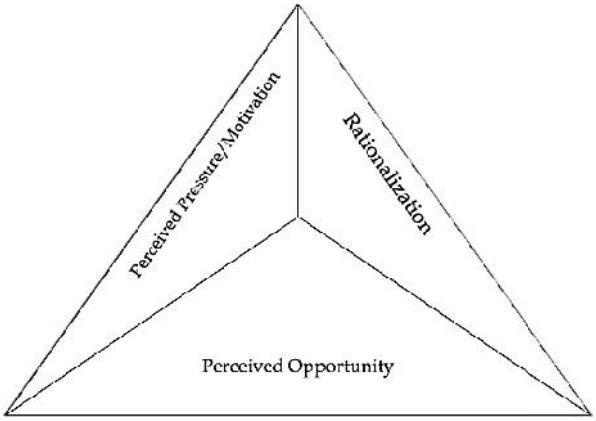
External fraud against an organization covers a broad range of schemes. A dishonest vendor might engage in a bid-rigging scheme, bill the company for goods or services not provided, or demand bribe from an employee.

**Examples**:

- A dishonest customer might submit a defective cheque or falsified account information for payment.
- Facing a threat of security breach and theft of intellectual property perpetrated by an unknown third party.

## 2.3 Fraud Triangle

Donald Cressey (1953), the famous criminologist, developed the concept of 'fraud triangle', citing the three elements of the triangle as: (1) motivation (pressure), (2) opportunity, and (3) rationalization. He described motivation as a non-shared financial problem, opportunity due to lack of internal control and rationalization as the ability of a person to rationalize his/her behavior. The fraud triangle is a framework commonly used in auditing to explain the reason behind an individual's decision to commit fraud.




The Fraud Triangle

### Motivation (Pressure, Incentive)

The motivation component of fraud is the pressure or 'need' that a person feels. In other words, it is the incentive or pressure to commit the crime or fraud. The motivation could also be a perceived financial need, whereby a person strongly desires some material goods, but does not have enough money or means to acquire them. Any pressure in one's business or personal life could conceivably motivate the person to commit a fraud. Most fraud experts believe that pressure can be divided into four main groups: (1) financial pressures, (2) vices, (3) work-related pressures, and (4) other pressures.

The following are the most common pressures that motivate the person to commit fraud:

### Financial Pressure

- Greed
- Living beyond one's mean
- High bills or personal debt
- Poor credit rating
- Significant personal financial losses
- Unexpected financial needs
- Inadequate income
- An overwhelming desire for personal gain

### Vice Pressures

Closely related to financial pressures are motivations created by vices such as gambling, drugs, alcohol and expensive extramarital relationship.

### Work-Related Pressures

- Strong challenge to beat the system
- A close association with customers
- Feeling of job-dissatisfaction
- Being overlooked for promotion
- Feeling underpaid

Possessiveness about custody or records/office space

### Other Pressures

- Where spouse or family insists on an improved lifestyle
- Undue family pressure or peer pressure

- Revenge
- Power dominance

**Caution:**One thing is for certain that eliminating pressures in the fraud triangle has an effect similar to the removal of heat from the fire triangle. Without some kind of pressure, fraud rarely occurs.

### Opportunity

The opportunity provides the method or circumstances of committing a crime or fraud. A perceived opportunity to commit fraud, conceal it, or avoid being punished is the second element of the fraud triangle. Management in an organization must understand the opportunity that could lead any person to commit fraud and then minimize the risk of fraud by reducing the opportunity that exists for such fraud. A person committing fraud abuses his position of trust to meet his greed, with a low-perceived risk of getting caught.

**Example:** If an employee has access to a blank cheque and has the way to reconcile the company's bank statement, he may see an opportunity to forge the cheque payable to himself. This indicates that the person has a perceived opportunity to commit fraud.

Some of the major factors and conditions that enable an individual to have the opportunity are:

- The weaknesses of the company's internal control systems;
- Access to accounting records or assets;
- Lack of supervision;
- Unethical behavior of top managers; and
- The belief that the person will not be caught
- Lack of an Audit Trial
- Excessive trust in certain employees
- Unprofessional environment
- Lack of appropriate separation of duties or independent checks.
- Inadequate management approval
- Inadequate system control
- Nexus with supplier
- Inadequate record keeping with respect to misappropriation of assets
- Poor physical safeguards over cash inventory or fixed assets Lack of mandatory vacations for employees holding key positions

### Rationalization

The third factor, which encourages the committing of a fraud, is the ability of the person to rationalize his or her own behavior. Without such rationalization, a person will not commit fraud, even if he has the motivation and opportunity. The sense of ethics, morality and the idea of right and wrong is what prevents some individuals from rationalizing their behavior.

It is a mental process by which an individual can come to an understanding in his mind, and to justify his or her act or acts. After having the opportunity and the motive elements of the fraud triangle met, many need to and do rationalize their actions as the last and final step in the fraud triangle.

According to the American Institute of Certified Public Accountants (AICPA), while the perpetrators must rationalize the crime to themselves, before they commit the crime, after the act has taken place, the rationalization can often be abandoned.

Thus, a fraud cannot be committed without some sort of rationalization, even when there is enough motivation and opportunity. There are many reasons to rationalize taking part in espionage and fraud or fraud against an organization.

**Examples:**Some individuals rationalize their committed fraud that it is for a good cause. They may rationalize that it is not for them, but rather for their religion and for God. Reasons of Frauds

Some of the major factors and conditions that enable an individual to have the rationalization are:

- Low moral character
- View of fraud as action less crime
- 'Rules do not apply to me'
- A strong desire to beat the system
- Sense of entitlement
- Lack of strong code of ethics

Nearly every fraud involves the element of rationalization. Most fraud perpetrators are first-time offenders who would not commit other crimes. In some way, they must rationalize away the dishonesty of their acts. Common rationalizations used by fraud perpetrators include the following:

- The organization owes it to me.
- I am only borrowing the money and will pay it back. Nobody will get hurt.
- I deserve more.
- It's for a good purpose.
- We'll fix the books as soon as we get over this financial difficulty.
- Something has to be sacrificed my integrity or my reputation. (If I don't embezzle to cover my inability to pay, people will know I can't meet my obligations and that will be embarrassing because I'm a professional.)

Certainly, there are countless other rationalizations. These, however, are representative and serve as an adequate basis to discuss the role of rationalization in the perpetration of fraud.

## 2.4 Reasons of Fraud

Motivation, Opportunity, and Rationalization are three important factors, which are connected with committing fraud. Motive comes from financial pressure; opportunity occurs through a weakness in internal control and rationalization is the fraudster's internal justification for his or her act. Competitive and economic survival can be a motive to commit a fraud. The white-collar crimes are not often committed by hardcore criminals; these are often committed by moral people who are under financial strain and distress. In committing a fraud, motivation has an important role as compared to opportunity to commit a fraud. People often commit fraud because they want to be wealthier and do not care about the consequences of their wrongful acts. Sometimes, frauds are committed by people to satisfy their ego or to maintain their false status.

The circumstances or reasons for committing a fraud can be categorized as (1) The lifestyle issues, and (2) Other issues.

### Lifestyle Issue

Greed for a noticeable change in lifestyle or obvious wealth, high debts, and other financial obligations.

### Other Issues

Personal problems, legal problems, addiction, criminal history, weak code of ethics, attempts to beat the system, questionable work habits- poor performance, overly protective of job duties, lack of transparency, poor management information, poor internal control systems of an organization, etc.

**CaseStudy:QuickBooks/Classic Lapping Scheme**

The small family business had been operational for nearly 30 years. At the end of their careers, the husband and wife owners relied heavily on their longstanding office manager

for all the financial activities of the business, except check-signing authority.

Following up on a discrepancy within a bank deposit identified by their accounting clerk, the owners discovered a difference between the deposit slip the office manager had completed and the actual deposit slip received by the bank after the office manager completed the deposit.

The original deposit slip included the names of four customers along with their payment amounts, two of which were in cash. The deposit slip received by the bank for that same day included the same dollar amount total, but was comprised of five (and not four) customer names and amounts. Two of the customer names were the same as reflected on the original deposit slip, but the two customers who paid cash had been replaced with different customer names. A fifth customer name had also been added.

Upon researching the payments received per the QuickBooks system maintained, it was quickly revealed that two large checks received were allocated in part to the customers who made the payments, and also in part to the two customers who paid in cash. The deposit total was accurate, but the composition was fraudulent. The scheme was clear—the office manager was skimming (stealing) the cash payments, and concealing her thefts by allocating payments from other customers to the cash paying customers' balances.

The office manager was terminated and was pursued criminally. The owners recovered a portion of the diverted funds when their insurance claim was filed and paid. A lack of records prevented them from determining just how long the office manager had been stealing, and how much they lost to her over the many years of her employment.

Source: Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). Forensic Accounting and Fraud Investigation (CPE ed.). John Wiley & Sons.

## 2.5 Psychology of Fraudster (Who Commits Fraud?)

Anyone can commit fraud, and fraudsters cannot be distinguished from other people by their demographic or psychological characteristics. Most fraud perpetrators have profiles that look like those of other honest people. From the definition, taxonomy, ingredients, and fraud triangle, one may conclude that fraud is caused mainly by factors external to the individual: economic, competitive, social, and political factors, and poor control mechanism. However, few persons are internally influenced to commit fraud specifically when it comes to satisfy their egos, addictions and psychology. Some people are more prone to commit fraud than others. Therefore, besides the external and internal environmental factors, the nature of people is more important consideration of committing fraud.

Gwynn Nettler, in his well-known book 'Lying, Cheating and Stealing', offers the following insights on cheaters and deceivers:

1. People who have experienced failure are more likely to cheat.

2. People who are disliked by others and who dislike themselves, tend to be more deceitful.

3. People who are impulsive, distractable, and unable to postpone gratification are more likely to engage in deceitful crimes.

4. People who have a conscience (fear, apprehension, and punishment) more resistant to the temptation to deceive.

5. Intelligent people tend to be more honest than ignorant people.

6. The Middle- and upper-class people tend to be more honest than the lower-class people.

7. The easier it is to cheat and steal; the more people will do so.

8. Individuals have different needs and therefore different levels at which they will move to lie, cheat or steal.

9. Lying, cheating, and stealing increase when people are under stress and to achieve important goals.

10. The struggle to survive generates deceit.

As per KPMG research in 2007 on the profile of a fraudster by analyzing from cases in Europe, India, the Middle East and South Africa and as per ACFE research on the profile of fraudster by analyzing fraud cases in US, the majority of frauds were committed by men and particularly by senior managers, including owners and executives, by employees working in organization for a long period and by those employees working in Finance Department. The type of person committing a fraud depends upon the nature of fraud. Misappropriation of assets fraud is committed by employees while financial statement frauds are committed by owners and executives.

As per KPMG research (2016) in Indian context on the profile of a fraudster, Indian fraudsters are young in age compared to global counterparts. They start early and one-fourth of the fraudsters were found to be in 1-4 years of service. Greed is the predominant motivation for Indian fraudsters. Weak controls are a large and growing problem, and present opportunities for fraud to take place in India. Collusive fraud is on the rise, and can involve internal employees as well as third parties. Technology is increasingly being used to enable frauds, and cyber frauds continue to emerge as a threat.

**Notes:** It is important to understand the characteristics of fraud perpetrators because they appear to be very much like people who have traits that organizations look for in hiring employees, seeking out customers and clients, and selecting vendors. This knowledge helps us to understand that (1) most employees, customers, vendors, and business associates and partners fit the profile of fraud perpetrators and are probably capable of committing fraud and (2) it is impossible to predict in advance which employees, vendors, clients, customers, and others will become dishonest. In fact, when fraud does occur, the most common reaction by those around the fraud is denial. Victims cannot believe that trusted colleagues or friends have behaved dishonestly.

## Summary

Fraud is a deception made for personal gain. It is an intentional act to induce another person to part with something of value or to surrender a legal right.

It can range from a minor theft by an employee to a large scale misappropriation of assets or manipulation of financial statements.

It can be committed for the organization or against the organization. It can be civil wrong or criminal wrong. It can be committed by an individual or in collusion.

It can be of many types viz. occupational fraud, employee fraud, vendor fraud, customer fraud, financial statements fraud, employee embezzlement, skimming and so on.

The fraud triangle is a framework commonly used in auditing to explain the reason behind an individual's decision to commit fraud.

Motivation, Opportunity, and Rationalization are three important factors, which are connected with committing fraud.

Motive comes from financial pressure; opportunity occurs through a weakness in internal control and rationalization is the fraudster's internal justification for his or her act.

Research shows that anyone can commit fraud, and fraudsters cannot be distinguished from other people by their demographic or psychological characteristics.

## Keywords

**Cash Larceny:**Cash larceny is the theft of cash or payment after it has been recorded.

**False Statement**: To make untrue statement about financial condition with an intention to deceive person whom statement is made.

**Falsify**: To make false statement by mutilation, addition or deletion in a document

**Forgery:**The crime of falsely making or changing a written paper or signing someone else's name.

**Fraudulent Concealment**: The deliberate hiding or suppression, with an intention to deceive or defraud any other persons, of a material fact or circumstances by a person, which he is legally bound to disclose

**Fraud:**It is a deception made for personal gain.

**Mens rea** : It is an intention to commit offence and is related to the mind of the offender.

**Misapplication**: The action of misapplying; improper, illegal, wrongful, or corrupt use or application of funds, property, etc.

Misappropriation: Appropriating an asset to improper use.

**Occupational Fraud or Management fraud**: The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

**Skimming:** The theft of cash or payments before they are recorded on the company books

**Wrongful gain**: It means the gain by unlawful means of property to which the person gaining is not legally entitled;

**Wrongful loss:** It means the loss by unlawful means of property to which the person losing is legally entitled.

## SelfAssessment

1. Fraud perpetrators:

A. Look like other criminals
B. Have profiles that look like most honest people
C. Are usually old
D. Are highly educated

2. Which of the following is not one of three element of fraud?

A. Perceived pressure
B. Perceived opportunity
C. Rationalization
D. Intelligence

3. Which of the following is a common perceived pressure?

A. The ability to outsmart others
B. Opportunity to cheat others
C. A financial need
D. The ability to borrow money by committing fraud

4. If pressures and opportunities are high and personal integrity is low, the chance of fraud is:

A. High
B. Medium
C. Low
D. Very low

5. Whichof the following is not a common type of fraud pressure?

A. Vices

B. Work-related pressure
C. Financial pressures
D. Pressure to excel others

6. Opportunity involves:
A. Opportunity to commit fraud
B. Opportunity to conceal fraud
C. Opportunity to avoid being punished for fraud
D. Opportunity to commit fraud, conceal fraud or avoid being punished for fraud

7. Which of the following is a common vice that motivates people to commit fraud?
A. Poor credit
B. Greed
C. Drugs
D. Improved lifestyle

8. "Deceptive manipulation of financial statement" describes which kind of fraud?
A. Employee embezzlement
B. Management fraud
C. Stock market fraud
D. Vendor fraud

9. Which of the following is not a form of vendor fraud?
A. Overcharge for purchased goods
B. Shipment of inferior goods
C. Non-shipment of goods even though payment is made
D. Not paying for good purchased

10. Which of the following is not a type of fraud?
A. Direct employee embezzlement
B. Indirect employee embezzlement
C. Investment schemes
D. Customer frauds

11. Which of the following deals with offenses of a public nature?
A. Civil law
B. Criminal law
C. Both civil and criminal law
D. None of civil and criminal law

12. Fraud is considered to be:
A. A serious problem that continues to grow
B. A problem felt by a few individuals, but not by most people

C. A mild problem that most businesses need not worry about
D. A problem under control

13. People who commit fraud are usually:
A. New employees
B. Not well groomed and have long hair and tattoos
C. People with weak personalities
D. Trusted individuals

14. Why does fraud seem to be increasing at such an alarming rate?
A. Digitalization and technology make fraud easier to commit and cover up
B. Most frauds today are detected, whereas in the past many were not
C. A new law requires that fraud be reported within 24 hours
D. People understand the consequences of fraud to organization and businesses

15. The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" is the definition of which of the following types of fraud?
A. Customer fraud
B. Vendor fraud
C. Management fraud
D. Employee embezzlement

## Answers for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | B | 2. | D | 3. | C | 4. | A | 5. | D |
| 6. | D | 7. | C | 8. | B | 9. | D | 10. | C |
| 11. | B | 12. | A | 13. | D | 14. | A | 15. | D |

## Review Questions

1. What is fraud? Discuss the key elements of fraud.
2. List and describe the different types of fraud.
3. What types of people commit fraud?
4. What motivates people to commit fraud?
5. What is the fraud triangle, and why is it important?
6. Explain the different types of pressures.
7. How does rationalization contribute to fraud?

## Further Readings

- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2009). *Forensic*

*Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.

- Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.
- Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). *Forensic Accounting and Fraud Investigation* (CPE ed.). John Wiley & Sons.

## Web Links

- https://metro.co.uk/2012/09/14/top-10-reasons-frauds-occur-3817555/
- https://corporatefinanceinstitute.com/resources/knowledge/accounting/fraud-triangle/
- https://studylib.net/doc/8103925/guide-to-preventing-workplace-fraud
- https://seon.io/resources/psychology-of-fraudsters-101/#:~:text=Some%20scammers%20pursue%20the%20lifestyle,deal%20with%20their%20self%2Dconsciousness.

# Unit 03: Corporate Fraud

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the meaning and nature of corporate fraud.
- illustrate the fraud for and against the company.
- evaluate the position of fraud perpetrators and victims in various corporate frauds.

## Introduction

Fraud reflects the relationshipbetween motivation, rationalization, and behavior. Fraud is an act of an individual(s) that can be civil or criminal. People claiming different cultural heritage differ in how they perceive fraud in general and in evaluating the specific type of frauds.

Corporate fraud can be for or against the company, as it is an intentional act, omission, or concealment of fact or information by any person to gain or injure the company's stakeholders for any wrongful gain or loss. Corporate culture is mainly responsible for the occurrence of any fraud. Unless a company embraces and demonstrates ethical conduct, it cannot grow and prosper in the long run. For the first time, the Companies Act 2013 inserted the concept of fraud under Section 447, and stringent penalty has been incorporated for those who indulge in fraud. This move of regulatory bodies further corroborates the importance of knowing the meaning, types, parties involved or affected, and mechanisms of corporate fraud. The present unit briefly discusses corporate fraud's nature, types, and victims.

## 3.1 Definition of Corporate Fraud

Fraud committed by or against a company is often referred to as corporate fraud or a white-collar crime. A company is an 'artificial juridical person,' invisible and intangible, created by law, with a discrete legal entity, perpetual succession, and a common seal. It is an association of various stakeholders: shareholders, investors, customers, employees, vendorpartners, governments, and society. The primary stakeholders of a company can be expressed in one word, 'SPICE,' where S stands for shareholders, P for the public at large, I for investors, C for customers, and E for employees. A corporation must be fair and transparent to its stakeholders in all its transactions. In a

globalized scenario, corporations need to access global resources, attract and retain the best human capital from various parts of the world, partner with vendors on collaborations, and live in harmony with the community. Unless a corporation embraces and demonstrates ethical conduct, it cannot grow and prosper for long. Based on the principle, 'As the ruler, so is the rule,' it is observed that people who know about management's wrongdoings or those who have assisted the management in committing fraud also tend to resort to fraud.

On the contrary, there are instances that,over time, some of the persons assisted will become whistleblowers and disclose the scam to the public. Corporate frauds have become a global phenomenon with the advancement of commerce and technology. India, a fast-developing country, has witnessed an enormous increase in corporate fraud in recent decades.

## 3.2 Fraud under the Companies Act; 2013

The Companies Act mainly regulates the corporate sector since different provisions have been provided for regulating a company's affairs.For the first time, the concept of fraud was inserted in the Companies Act 2013.

Regardless of the definition, specific characteristics are common to all types of fraud. These are:

1. It is a misrepresentation of a material fact.

2. It is made knowingly and deliberately.

3. It is made with the intent to deceive.

4. The victim must have relied on the misrepresentation.

5. It results in injury or damage to the victim.

As per Section 17 of the Indian Contract Act 1872,

Fraud means and includes any of the following acts committed by a party to a contract with an intent to deceive the other party to it or to induce him to enter into a contract:

- The suggestion as a fact of that which is not true by one who does not believe it to be true;
- The active concealment of a fact by one having knowledge or belief of the fact;
- A promise made without any intention of performing it;
- Any other act fitted to deceive;
- Any such act or omission as the law specifically declares to be fraudulent.

**Essential elements of Fraud**

- The representation or assertion must be false.
- The representation or assertion must be of a fact.
- There must be an intention to deceive the other party.
- Fraudulent act must be committed with the knowledge of its falsity.
- Fraudulent act must be done by a party to the contract or his authorized agent.
- Fraudulent act must have deceived the other party.

**Example:**Maggie, a seller of a horse, says that the horse is a "Beauty" and is worth 5 lakh. It is merely Maggie's opinion. Thus, it will not act as a fraud. But if Maggie paid only 2 lakh for it, then he has misstated a fact and will be considered fraud on the grounds of Representation or assertion must be a fact.

Legal provisions have been made for preventing and curbing corporate fraud under Section 447 of the Companies Act, 2013, which defines fraud as:

Without prejudice to any liability, including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud [involving an amount of at least ten lakh rupees or one percent of the turnover of the company, whichever is lower] shall be punishable with imprisonment for a term which shall not be less than six months but which may

extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud:

Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.

Provided further that where the fraud involves an amount less than ten lakh rupees or one percent of the turnover of the company, whichever is lower, and does not involve public interest, any person guilty of such fraud shall be punishable with imprisonment for a term which may extend to five years or with fine which may extend to fifty lakh rupees or with both.

Explanation.

(i) "fraud," concerning affairs of a company or anybody corporate, includes any act, omission, concealment of any fact, or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

(ii) "wrongful gain" means the gain by unlawful means of property to which the person gaining is not legally entitled;

(iii) "wrongful loss" means the loss by unlawful means of property to which the person losing is legally entitled.

The definition of 'fraud' can be broken up into various building blocks as follows:

- Any act or omission to act
- Fraudulent concealment
- Abuse of position
- By any person
- Intent
- Injury
- Wrongful gain and wrongful loss

### Any act or omission to act

An act means to take action or to do something. Mere coming of an idea into mind to commit fraud does not amount to fraud until the idea is converted into an act. An act of omission is the failure to perform an act expected to be done by a person, whereas the act of commission is doing an act that causes harm.

According to Oxford Law Dictionary, the word omission means "a failure to act." In other words, it is called an omission when a person is bound to do an act but omits it or deliberately neglects it.

A summary of criminal law on omissions: a defendant is only guilty of a crime when failing to act, where he or she is under a duty to act.

 Example

If a person passing by a pool sees a child drowning in it and there is no other source to rescue him from drowning, and that person passes by that pool and leaves the child to die, he commits an omission.

There is actus rea, also called the act of the offender. It is related to doing or acting on a particular act. As far as omission is concerned, it is omitting an act that a person is bound to do or act.

In the UK, no specific laws are described to punish a person who omits to do or omits to act unless and until he is duty-bound to do such an act. This is not the same as the owing duty of care, but generally, 'where there is a duty to act, there is almost inevitably a duty of care. Certain people owe a duty towards others, such as mother and father owe a duty towards their children, partners living together in the same dwelling, and the duties a doctor owes toward his patients.

These are not statutory duties. These are, in fact, a kind of moral duties because these are not specified in any law or statute.

In the case of Barendra Kumar Ghose AIR (1924), it was pronounced that the legal consequences of an 'act' and of an 'omission' are the same; if an act is committed partly by an act and partly by an omission, the consequences will be the same as if the offense was committed by an 'act' or by an 'omission' alone. This does not create a substantive offense. This shows that when an offense is an effective part of an act or part of an omission, it is one offense only.

### Fraudulent Concealment

The word 'Fraudulently' in Section 206 of the Indian Penal Code, 1860 can be interpreted as nothing more than 'dishonestly.' A dishonest act is not a fraudulent act unless and until an intention to deceive is present in that dishonest act. Where there is neither an intention to deceive nor secrecy, the dishonest act is not fraudulent. [1937 MWN 462: 46LW139: AIR 1937 Mad 713: (1937) 2 MLJ 802.]

The word 'concealment' in Shorter Oxford English Dictionary, 3rd Edition, is intentional suppression of truth or fact, known to injure or prejudice another. Fraudulent concealment means the deliberate hiding or suppressionof a material fact or circumstances by a person he is legally bound to discloseintending to deceive or defraud any other person.

 **Examples:**

- Failure to disclose defects in goods
- Omitting assets from the bankruptcy schedule to keep them from being available for distribution to creditors.

Fraudulent misrepresentation is also a part of fraudulent concealment. A misrepresentation is made with the express intention of defrauding someone, which subsequently causes injury to that person. For a statement to be deceitful, it must be untrue, made with the knowledge of its falsity, or made in reckless disregard of the truth. The misrepresentation must be such that it causes harm to another individual. Deceit is the quality that prompts intentional concealment or perversion of truth to mislead. The tort or fraudulent representation of a material fact made with the knowledge of its falsity without reasonable grounds for believing its truth and with intent to induce reliance on it, and the plaintiff justifiably relies on the deception to his injury.

### Abuse of Position

In many cases, the most serious frauds and corruption frauds are committed by people at the top who have the power to conduct fraudulent transactions and cover them up. Several things suggest that someone is abusing his position and could be committing fraud in reality.

 **Example:**

An employee creates patient records on the patient booking system for a family member who lives abroad to enable them to access National Health Services free of charge.

Fraud by abuse of position is defined in Section 4 of the Fraud Act, 2006 (UK), which reads:

Section 4:Fraud by abuse of position

1. A person is in breach of this section if he

(a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,

(b) dishonestly abuses that position, and

(c) intends, by means of the abuse of that position

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

2. A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

### By any Person

The Companies Act has not defined the concept of a person, while the meaning of a person is defined under Section 11 of the Indian Penal Code, 1860. Every person charged for committing a

crime in India is liable for punishment regardless of caste, religion, creed, sex, or color. However, the Criminal Courts cannot try any proceeding against certain persons, which include:

1. Acting President and Governors.

2. Foreign Sovereigns; and

3. Ambassadors, Companies, and Corporations.

Companies are excluded since these entities are artificial juridical persons, and their acts are performed by individuals or a group of individuals. Therefore, the criminal courts are exempted from awarding any punishment of imprisonment to a company, but a fine can be imposed on a company or corporation. Further, a company can be prosecuted and convicted under different enactments, like the Prevention of Food Adulteration Act 1954 and the Essential Commodities Act 1955. But a company or corporation cannot be prosecuted for an offense committed by an individual alone, for example, murder and dacoity. These entities cannot be indicted for compulsorily punishable offenses with imprisonment. Except this, they can be held liable for the criminal acts or omissions of its directors, employees, or authorized persons.

### Intent

An act of fraud, omission, or concealment should be done with an intent: (1) to deceive; (2) to gain undue advantage from someone; and (3) to injure the interest of (i) the company, (ii) a shareholder, (iii) creditor, or (iv) any other person.

The main emphasis of this definition is on 'intent.' The legal system in India is replete with concepts like 'intent,' 'public interest,' and 'principles of natural justice. This is particularly true about the Indian Penal Code and certain other legislations. The term 'intent' is of paramount importance. It is the 'intent' of a person which will determine whether his action, omission, concealment of facts, or abuse of position amounts to fraud or not.

A person's intent must be to deceive, gain undue advantage, or injure the other party's interest. Deceive is to induce someone to believe that a thing is true, which is false, and the person who is deceiving knows or believes it is false. The other party can be a company, its shareholder, creditor, or 'any other person (associated with the company concerned). In most criminal cases, the main element involved is mens rea, which is an intention to commit offence and is related to the offender's mind.

### Injury

The word "injury" denotes any harm illegally caused to any person in body, mind, reputation, or property. The word 'injury' has been given a wide meaning. It will include every tortious act. Thus unlawful detention of a cart at a toll gate caused by an illegal demand for payment of toll amounts to injury. A threat of a decree which can never be executed is a threat of harm to an individual in his person, reputation, or property. A threat to use the process of law to enforce payment of more than is due is illegal, and such an object is a threat of injury.

### Wrongful Gain and Wrongful Loss

It is immaterial whether or not there is any 'wrongful gain' or 'wrongful loss.' The expressions 'wrongful gain' and 'wrongful loss' have also been defined in the Act. While 'wrongful gain' has been defined as the gain by unlawful means of any property to which the person gaining is not legally entitled, 'wrongful loss' means the loss by unlawful means of any property to which the person is legally entitled.

## 3.3 Nature of Corporate Fraud

Corporate fraud is non-negotiable in nature that adversely affects the interest of the stakeholders. There are numerous consequences of a corporate fraud. Important among them are:

1. Financial loss.

2. More Government control due to non-compliance and regulatory infringements.

3. More litigation.

4. Adverse publicity by the media by labeling it as a scam or scandal.

5. Damage to the personal reputation and career of those employees and managers who were not involved in the fraud; and

6. Disruption to the business can result in a company's liquidation.

A company, being a separate legal entity, has high credibility in the eyes of the persons concerned. Because of the special legal status and consequent respect it commands, a company grows steadily. The basic truth lies in the fact that corporate frauds are shielded behind the "Corporate Veil" facade." A company works under various legal and statutory requirements mainly intended to protect the stakeholders. Since human beings and human conduct run a company is very individualistic, the conduct of a company is the aggregate of the conduct of the individuals managing its affairs.

Since the industrialization of India, there have been cases of corporate frauds of diverse nature - stock market fraud, mass-scale cheating of investors and shareholders, companies vanishing into thin air, deliberately making a company sick and putting it before the Board of Industrial and Financial Reconstruction, or bringing it under liquidation before the High Court, could all be different ways of committing corporate fraud. The insiders often initiate corporate fraud with the help of certain unscrupulous professionals and consequent non-monitoring by Governmental agencies. Like cancer, corporate fraud generally comes to light suddenly, with little time left for investors and government agencies to take any preventive or curative action. According to N. Vittal, the legendary Chief Vigilance Commissioner of India, during his inaugural address at DMA-PWC Seminar on "Corporate Frauds Overview, Detection and Prevention" in New Delhi on 26.02.2002, the three dimensions of any corporate fraud are:

(1) the human dimension,

(2) the technology dimension; and

(3) the legal dimension, which are briefly explained below:

**(1) The human dimension**

Insiders are the main perpetrators to commit corporate fraud. Insiders are mainly dedicated employees who never take leave, and when they fall sick, and somebody else looks into what the dedicated employee was doing, it is found that he had been perpetrating a regular fraud by fiddling around with the accounts.

**(2) The technological dimension**

The second dimension of corporate fraud is fast-changing technology. The technology has two dimensions to prevent fraud and to pamper fraud. The -- major risks of IT would be

(a) Environment risks,

(b) IT operations risks, and

(c) IT product risks.

**(3) The legal dimension**

The third dimension which encourages corporate fraud is the failure of the regulatory mechanism and inadequate legal penalty. The Sick Industrial Companies Act and the Board of Industrial and Financial Reconstruction have been thoroughly misused by corrupt people and fraudsters to take advantage at the cost of the public interest. It is imperative to strengthen the regulatory mechanism and to provide an adequate penalty to deter scams. Corporate frauds are generally (1) highly complex, (2) the result of a web of financial transactions used to commit fraud, and (3) based on human ingenuity.

## 3.4 Frauds for and against the Company

Any fraud perpetrated by, for, or against a company is known as corporate fraud. Corporate frauds are often intended to satisfy the economic needs of a company's officials or executives whose compensation is based largely on one performance measure.Corporate fraud is intended to benefit the organizational identity or to harm the entity. Frauds against the company are intended to benefit only the perpetrator. In frauds directed against the company, the victim is a company, while in frauds for the company, the company is a beneficiary.

**Corporate fraud for and against the company**

| For the company | Against the company |
|---|---|
| By Employers<br>1. Escalating profits by:<br>- Overstating sales,<br>- Understating expenses, and<br>- Not recording sales return<br>- Not recording non-operating losses<br>2. Window-dressings of Financial position by:<br>- Overstating assets<br>- Understating liabilities<br>- Showing fictitious assets<br>3. Price fixing<br>4. Cheating customers through:<br>- Misleading advertisement<br>- Manipulating quantity<br>- Substituting cheaper materials for producing the product<br>- Charging high for low-valued or quality product<br>5. Violating government regulations by:<br>- Political corruption<br>- Evasion of taxes<br>- Padding cost on government contracts. | By Employees<br>1. Misappropriation of assets<br>2. Forge signatures and endorsement of negotiable instruments<br>3. Manipulation of receivables through:<br>- Fake vendor invoices<br>- False expense vouchers<br>- Fake suppliers<br>- Fake contracts<br>4. Manipulation in employee cost through:<br>- Payment to bogus employees<br>- Less payment to employees<br>- Excess salary to senior executives who are relatives of owners<br>By vendors<br>1. Short shipping of goods<br>2. Substituting goods of inferior quality<br>3. Overbilling or double-billing by vendors, suppliers, and contractors<br>4. Price fixing |

Source: Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.

## 3.5 Victims of Corporate Fraud

The most trusting people are also the most susceptible and victims of fraud. This rationale postulates that organizations with the highest control level are the least susceptible to fraud. But it does not lead to the conclusion that frauds are not committed in organizations with high controls. Owners, employees,and even outsiders commit fraud, affecting certain persons. People become the victim of corporate fraud outside or inside the company. The insiders, including the directors, managers, and employees, may suffer a loss of position, reputation, or standing. The outside victims include investors, creditors, partners, customers, suppliers,underwriters, attorneys, and independent auditors. In Corporate fraud, we can study the victim of fraud as fraud committed by whom, which type of fraud is committed, and who is the victim of fraud. These persons can be categorized as

**(1) Frauds committed by**

- Company and its Directors
- Competitors
- Employees and Employers
- Suppliers/Vendors/Contractors

**(II) Types of Frauds**

- Bribery and Corruption
- Corporate Espionage
- Financial Statement Fraud
- Misappropriation of Assets
- Procedure-Related Fraud

### (III) Victim or Affected Persons

- Bankers
- Competitors
- Customers
- Employers
- Employees
- Government Agencies
- Insurance Agencies
- Stakeholders

The list of fraud perpetrators, victims, and fraud types

| Type of Frauds | Fraud Perpetrator | Victims |
|---|---|---|
| False or Manipulated financial statements, False financial forecasts, False representations, Fraudulent financial reporting,and False credit applications. | Company and its Management (Directors) | Stakeholders (Shareholders, Creditors, Investors) |
| Fraudulent loss claims, Arson for profit or economic Arson, False Insurance claims,Workers' compensation fraud | Company and its Management (Directors) | Insurance Agencies |
| False reports/returns, False claims, Contract Padding, Wilful failure to file reports/returns | Company and its Directors | Government Agencies, Income tax authorities, Regulatory bodies like SEBI, RBI |
| False employment applications, False benefit claims, False expense claims, Theft and Pilferage, Fake performance, Embezzlement, Corruption, Worker's Compensation (Working while collecting workers' compensation benefits, Faking injury, Claiming to be injured at work when the injury occurred elsewhere) | Employees and Employers | Company as a whole, Employers, Insurance companies |
| Expense account padding, Fake performance, Overstating revenue, Overstating assets, Overstating profits, Understating expenses, Understating liabilities, Theft of assets, Embezzlement, Commercial bribery, Insider trading, Related party transactions, Manipulation of records, Destruction of records | Vendors, Suppliers, Contractors, Employees | Employers |
| False advertising, False Weights, False measures, False representations, False labeling/branding, Price fixing, Quality substitution, Defective products, Short shipment, Overbilling, Double billing, Substitution of inferior goods | Company and its Directors, Vendor | Customers |

| | | |
|---|---|---|
| Predatory/Exploitative Pricing, Selling below cost to eliminate or prevent competition, Information piracy, Infringement of patents/copyrights, Theft of trade secrets, Corruption of employees | Company and its Directors, Competitors | Competitors |
| False applications for credit, False financial statements for enhancement of credit facilities | Company and Directors | Bankers |
| Misappropriation of Assets, Cash Embezzlement | Employees | Company |

Source: Adapted from G Jack Bologna, Robert J. Lindquist (1995), Fraud Auditing and Forensic Accounting, New Tools and Techniques (New York: Wiley)

**Caution:**Improper revenue recognition is the most common technique used by management to misstate financial information.

**Notes:**

Expense account padding: To make unnecessary or fraudulent charges to one's company expense accounts for personal use.

Employee theft and Pilferage: Internal theft also is referred to as employee theft, pilferage, embezzlement, fraud, stealing, peculation, and defalcation. Employee theft is stealing by employees from their employers. Employee theft involves stealing money, time, and merchandise from the workplace for personal gain. Pilferage is stealing in small quantities or stealing items or things of little value.

**Examples:**

Employee Theft: Stealing Cheques, Taking money from a petty cash box before it is recorded, and data theft.

Pilferage: Stealing inventory items in small quantities, stealing less valued items of inventory.

Workers' compensation fraud: Employers who misrepresent their payroll or the type of work carried out by their workers to pay lower premiums are committing workers' compensation fraud. Some employers also apply for coverage under different names to foil attempts to recover monies owed on previous policies or to avoid detection of their poor claim record.

**Examples:**

- Employer under-reporting payroll and number of employees to obtain a lower premium
- Intentionally misclassifying employees' job codes

**Did you know?**

What is Arson for Profit?

Arson for profit, or economic Arson, is when businesses or individuals set fires to reduce financial loss, recoup initial investments, or dispose of depreciated assets, usually for a payout from insurance companies.

Commercial Bribery: It means offering, paying, promising, or giving, directly or indirectly, anything of value to another company's agent, representative, intermediary, or employee, without that company's knowledge and consent, with the intent to influence the recipient's action concerning his company's business.

Insider Trading: Insider trading involves trading in a public company's stock by someone with non-publicmaterial information about that stock for any reason.

## Summary

- Fraud committed by or against a company is often referred to as corporate fraud or a white-collar crime.
- Fraud means and includes any of the following acts committed by a party to a contract with an intent to deceive the other party to it or to induce him to enter into a contract:
- ✓ The suggestion as a fact of that which is not true by one who does not believe it to be true;
- ✓ The active concealment of a fact by one having knowledge or belief of the fact;
- ✓ A promise made without any intention of performing it;
- ✓ Any other act fitted to deceive;
- ✓ Any such act or omission as the law expressly declares to be fraudulent.
- There are numerous consequences of a corporate fraud. Important among them are:

  1. Financial loss;

  2. More Government control due to non-compliance and regulatory infringements;

  3. More litigation;

  4. Adverse publicity by the media by labeling it as a scam or scandal;

  5. Damage to the personal reputation and career of those employees and managers who were not involved in the fraud; and

  6. Disruption to the business can result in a company's liquidation.

- The three dimensions of any corporate fraud are: (1) the human dimension, (2) the technology dimension, and (3) the legal dimension.
- Corporate frauds are often intended to satisfy the economic needs of a company's officials or executives whose compensation is mainly based on one performance measure.
- Frauds against the company are intended to benefit only the perpetrator.
- In frauds directed against the company, the victim is a company, while in scams for the company, the company is a beneficiary.

## Keywords

**Commercial Bribery:** It is a form of bribery involving corrupt dealing with potential buyers' agents or employees to secure an advantage over business competitors.

**Contract Padding:** When parties to a contract put unnecessary information in the contract to make it longer and harder to understand for committing fraud.

**Employee Theft**: It is characterized as any stealing, use, or misuse of an employer's assets without permission

**Expense Account Padding**: To make unnecessary or fraudulent charges to one's company expense accounts for personal use.

Misappropriation of assets:

**Pilferage**: Pilferage is generally an act of stealing items or things of little value. It can be seen from two main aspects: inventory and marine thefts.

**Workers Compensation Fraud**: When employers misrepresent their payroll or the type of work carried out by their workers to pay lower premiums.

## SelfAssessment

1. Who is most likely to perpetrate fraudulent financial reporting?

A. Members of the Finance Department
B. Production Employees
C. Management of the company
D. The internal auditors

2. Misappropriation of assets is generally perpetrated by:

A. Board of Directors
B. Management of the company
C. Employees at lower levels of the organization
D. The internal auditors

3.Which is the most common technique used by management to misstate financial information?

a) Overstatement of expenses
b) Improper revenue recognition
c) Understatement of liabilities
d) Understatement of assets

4. Fraudulent financial reporting may be accomplished through the manipulation of:

a) Assets
b) Revenue and expenses
c) Liabilities
d) Assets, revenue, expenses and liability

5. _____ is fraud that involves theft of an entity's assets.

A. Fraudulent financial reporting
B. A "cookie jar" reserve
C. Misappropriation of assets
D. Income smoothing

6. Which of the following is Not the characteristic of common fraud?

A. Misrepresentation of a material fact.
B. It is made unknowingly.
C. It is made with the intent to deceive.
D. The victim must have relied on the misrepresentation.

7. The following is an essential element of fraud.

A. The representation or assertion must be accurate.
B. The representation or assertion must be of an opinion.
C. There must be an intention to deceive the other party.
D. The fraudulent act must be committed innocently.

8. Fraud is more prevalent in large businesses than small businesses and non for profit organizations.

A. True
B. False

9. _____ denotes any harm illegally caused to any person in body, mind, reputation, or property.

A. Deceipt
B. Injury
C. Padding
D. Intent

10. _____defined as the gain by unlawful means of any property to which the person gaining is not legally entitled.

A. Profit
B. Gain
C. Wrongful Gain
D. Wrongful right

11. The cashier of Hitachi Delhi Ltd. receives cash from the customers but does not deposit all collected cash in the company's bank account. He keeps some cash in his pocket for personal use and does not put the entry of the cash receipt from a customer in the books of accounts. He is committing fraud by:

A. Abusing of position
B. Omission of Act
C. Misrepresenting
D. Injury

12. Manipulation of receivables through Fake vendor invoices is an example of:

A. Fraud for company
B. Fraud against company

13. Escalating profits by overstating sales is an example of:

A. Fraud for company
B. Fraud against company

14. Which of the following is an example of fraud for the company?

A. Short shipping of goods
B. Substituting goods of inferior quality
C. Misappropriation of assets
D. Misleading advertisement

15. Which of the following is an example of fraud against the company?

A. Price fixing
B. Window-dressings of Financial Position
C. Escalating profits
D. Violating government regulations

## Answer for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | C | 2. | C | 3. | B | 4. | D | 5. | C |
| 6. | B | 7. | C | 8. | B | 9. | B | 10. | C |
| 11. | A | 12. | B | 13. | A | 14. | D | 15. | A |

## Review Questions

1. Explain the concept of fraud under the Companies Act 2013.
2. Write short notes on the following:
   a) Any act/Omission to act
   b) Fraudulent concealment
   c) Abuse of position
   d) Injury
   e) Wrongful gain and Wrongful loss
3. Explain the nature of corporate fraud.
4. Illustrate frauds for and against the company.
5. Summarize the victims of different corporate scams.
6. What do you mean by corporate fraud? Explain its types.
7. Summarize the perpetrators of different corporate frauds.

## Further Readings

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2009). *ForensicAccounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.

Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.

Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). *Forensic Accounting and Fraud Investigation* (CPE ed.). John Wiley & Sons.

## WebLinks

https://corporatefinanceinstitute.com/resources/knowledge/finance/corporate-fraud/

https://www.attorneygeneral.gov/protect-yourself/insurance-fraud/types-of-insurance-fraud/

# Unit 04: Types of Corporate Fraud

CONTENTS



## Objectives

After studying this unit, you will be able to:

- Illustrate the different types of corporate fraud.
- Review the modus operandi of various corporate frauds.

## Introduction

Corporate fraud may be of different types encompassing the various activities and legal procedures involved. Corporate fraud can be committed internally or externally in a company by employees, customers, vendors, management, the Chief Financial Officer, the Board of Directors, and/or any other functional head. While an internal fraud is a fraud occurring within the organization and is committed by employees or the Board of directors, an external fraud is a fraud committed by outsiders. As per the research studies and expert surveys, corporate fraud can be divided into five categories as shown below:

- Bribery and corruption;
- Misappropriation of assets;
- Fraud through manipulation of financial statements;
- Procedure-related fraud;
- corporate espionage;
- Digital and e-commerce frauds

Let's understand the aforesaid corporate frauds in brief ahead.

Case study Enron Scam

One of the most notorious cases of corporate fraud is the Enron scandal. At its height, Enron, a major energy company, was raking in billions upon billions in profits. However, when the company began to face declining revenues and debt troubles, company executives hid the facts through massive accounting fraud.

In the end, both Enron and its accounting firm, Arthur Andersen, went under. Thousands of employees lost their jobs, and Enron's creditors and investors lost billions.

The Enron accounting scandal is credited with resulting in the passage of the Sarbanes-Oxley Act, which required more transparency in companies' financial reporting and imposed significantly harsher penalties on any company caught committing accounting fraud.

## 4.1 Bribery and Corruption

Bribery involves giving or receiving something of value to influence a transaction. Bribery and corruption are either in cash or in kind and include procurement fraud. Procurement fraud is a subset of bribery and corruption schemes. It is essentially the manipulation of the process of obtaining a contract for goods and services or obtaining an approval from a government agency or even getting a favorable order from the judge. Bribery is paying someone to do something illegal, corruption is taking a bribe to do the illegal act and fraud is doing an act intentionally which against the law. The manipulation is generally aimed at gaining an advantage in the bidding or proposal process, and such acts can range from an unfair use of insider information to the use of nefarious means to influence the process.

Did you know How can procurement fraud arise?

Procurement fraud can arise out of the following:

(1) Collusion between Employees and Vendors: It includes kickbacks, bid rigging, gifts, or other enticement provided by the vendor.

(2) Vendor's Fraud against the Company: A vendor might commit a fraud against a company by substituting goods of inferior quality, overcharging the company, engaging in false billing, or over-invoicing.

(3) Collusion between or among Vendors: Vendors might collude to artificially inflate the prices of goods and services in bids or proposals, or to help one another receive certain contracts based on an agreement between them

Bribery refers to the offering, giving, receiving, or soliciting anything of value to influence an 'official act', where 'official act' means the payments made to influence the decision of a government agent or employee. Simply, a bribe means to give, offer or promise to give money or something to a person in power to induce that person to do a certain act. Corruption is the dishonest or illegal behavior of powerful people. Corruption is a wider concept which includes bribery also. Corruption can be categorized as bribery, economic extortion, illegal gratuity, and conflict of interest.

*Notes*

**Economic Extortion** refers to forcing someone to do a particular act to give some favour to him.

*Example*

A factory manager started his own business and forced the vendors to divert some of their business to his own company if the vendor wanted to be associated with the company. If the vendor does not divert some business to the company, then his contract with the company would be cancelled and in such a case, the vendor is forced to transfer some business.

**Illegal Gratuities** also amount to a kind of bribery but in such cases, the intention is not present to influence some decisions. No direct money is involved in these cases, rather some benefit is offered to a person.

*Example*

A senior employee on behalf of the company negotiates with some parties to allot different work at the site of the company and in return for that, the party offered a 5-days foreign trip to an employee

along with family. Mere accepting this offer tantamounts to illegal gratuity as it can influence the decision of an employee.

While in **Conflict of Interest**, an employee, manager, or executive has an undisclosed economic or personal interest in a transaction that adversely affects the organization.

### Modus operandi of Bribery and Corruption

The modus operandi of bribery and corruption is briefly described below:

### Modus operandi in cash or kind type of Bribery

Fraud perpetrators use different methods to give bribes, a few of them are stated below:

***(1) Kickback:*** In the kickback scheme, a conspiracy develops between a vendor and an employee of the victim company.

*Example*

The purchase manager of the victim company orders goods to an existing vendor while the management of the company has clearly given instructions to divert some orders to new vendors. The purchase manager in return gets some percentage of the profit from the vendor by giving such an order to him.

***(2) Diverting Business to Vendor:*** An employee-fraudster directs more business to a party, against which he receives something in cash or in kind.

*Example*

The president of a supplier company offers some shares of his company to an employee of a purchaser company against the awarding of a substantial contract.

***(3) Over-invoicing***: In over-invoicing cases, the fraudster either has 'approval authority' or is a trusted employee of the employer. He being in the capacity of approval authority, make payment of inflated invoices or fraudulent invoices and in return gets back the percentage in the inflated or fraudulent invoice. Such schemes are also successful when the senior is forced to rely on the subordinate's guidance in purchasing matters.

### Modus operandi in Procurement type of Business

Like receiving cash or offering some benefits, fraud perpetrators have different strategies, to commit fraud. These Strategies are:

(1) Bid-Rigging Schemes: The competitive bidding process, in which several suppliers or contractors try to get contracts and the benefit of "inside influence," can ensure a vendor gets a contract after payment to the employee for this influence. The number of types of Bid Rigging schemes is described below:

***(a) Need Recognition Scheme:*** In this scheme, a comparison is drawn between an employee of the buyer's company and a contractor whereby an employee receives something of value as a result the victim company purchases unnecessary goods or services from the supplier at the direction of the corrupt employee.

***(b) Specifications Scheme:*** The specifications of a contract include lists of the elements, materials, dimensions and other relevant requirements for the completion of the project. Specifications are prepared to assist vendors in the bidding process. The employee is convinced by the vendor in the preparation of specifications for the contract on receipt of some money and tailors the specifications as per the capabilities of a particular vendor.

***(c) Bid Pooling:*** Bid pooling is a process in which several bidders conspire to split contracts up and ensure that each gets a certain amount of work. Instead of submitting confidential bids, the vendors discuss what their bids will be, so they can guarantee that each vendor will win a share of the purchasing company's business.

***(d) Fictitious Suppliers:*** Another way to eliminate competition is to solicit bids from fictitious suppliers. In such cases, the supplier in connivance with an employee of the company submits quotes in the names of several different fictitious companies to demonstrate price reasonableness on the final contract and these quotes are given in the fictitious names to validate his actual prices.

*Did you know* How do bribery and corruption impact the performance of stock markets?

Bribery and corruption impact the performance of a stock market by increasing volatility and deterring institutional investors from making long-term investments. Corruption can erode the very pillar of economic growth and could impact the valuation of a company, thereby denying the shareholders of a fair price. It increases the overall cost of conducting business as capital is borrowed at a higher cost. The biggest impact of corruption on business is its tendency to skew the level-playing field and attract organizations with the lesser capability to execute projects.

*Caution*

Bribery is a serious economic crime as it adversely affects the country's economic development. It promotes inefficiency in the utilization of resources, distorts the market, compromises quality, harms the environment and dents the moral fabric of the country.

## 4.2 Misappropriation of Assets

Asset misappropriation includes the misuse or theft of assets belonging to a company. Asset misappropriations can be divided between cash schemes and non-cash schemes. Cash schemes simply involve the theft of money, via cheques, money orders, or paper currency; they can be further divided between schemes focusing on cash receipts, and those related to cash disbursements. Non-cash schemes involve all other thefts of assets, such as inventory, equipment, supplies, or information.

The theft of cash, either by way of a cheque or currency, can be (1) skimming, which is stealing the funds before they are recorded in the books of the company, and (2) cash larceny, which is the theft of funds after the transaction has been recorded.

### Modus Operandi of Misappropriation of Assets

The company adopts different modes of theft of inventory and other assets to commit fraud. The assets may be categorized as 'tangible assets' and 'intangible assets'. The modus operandi of theft of these assets is depicted in the following table:

| Modus Operandi of Misappropriation of Assets | |
|---|---|
| Tangible Assets | Intangible Assets |
| 1. Fake Sales<br>2. Asset Requisition and Transfer<br>3. False Billing Scheme<br>4. False Incoming and Outgoing Inventory<br>5. Alteration in Inventory Records<br>6. Fictitious Sales<br>7. Writing off of Inventory and Other Assets<br>8. Physical Padding | 1. Mis-utilization of Information<br>2. Misappropriation of Securities<br>3. Manipulation of Pay-Rolls |

[Source: Adapted from Wells, J. T. (2011), Corporate Frauds Handbook, Prevention and Detection (New Jersey: Wiley)]

*Notes*

***Fake Sales:*** A fake sale occurs when goods are sold but not taken on record. Two people participate in this transaction, one company employee and the other an accomplice. The employee does not record the sale while the accomplice takes the assets without making any payment. The buyer passes a nominal amount to the employee to complete the illegal transaction.

***Asset Requisition and Transfer:*** In Asset Requisitions and Assets Pilfration, non-cash assets are moved from one location to another to facilitate the misappropriation of assets. They simply overstate the amount of assets and pilfer the excess. Fraudsters fabricate a project with a requirement of certain assets and these assets are those assets which they want to steal. These

frauds are committed by dishonest employees who falsify asset transfer forms and remove inventory or other assets from a warehouse. After transferring the assets, the fraudsters take them to their place.

***False Billing Scheme:*** A fraudster causes his company to purchase needless goods by false billing scheme; the company pays for those assets for which it has no use. For instance, the manager ordered the crockery items which were required for him, not for office purposes.

***False Incoming and Outgoing Inventory:*** In the case of false incoming consignments, the employee of a company, in connivance with other employees, manipulates the quantity of incoming goods as incoming goods are shown as short received while the goods are received in full quantity. This is done to steal those goods which are shown as short delivery. In false outgoing goods, the employee intends to steal the goods legally by creating false shipping documents and sales documents so that the stolen goods should be shown against sales.

***Alteration in Inventory Records:*** The perpetual inventory record matches with the physical inventory count which is also called as a forced reconciliation of the account. The perpetrator changes the numbers in the perpetual inventory to make them match with inventory in hand.

***Fictitious Sales***: Fraudsters create fake sales bills to mask the theft of assets and enters debit to accounts receivable, or corresponds to credit sales account to make it appear that the missing goods had been sold.

***Writing off of Inventory and other Assets:*** Removal of assets may be done by writing off of inventory and other assets. This removal may be before, or after they are stolen. A director disposed of fixed assets by reporting them as broken, while the assets were never broken but taken away by him for himself.

Writing off inventory and other assets is a relatively common way for fraudsters to remove assets from the books before or after they are stolen.

***Physical Padding:*** Manipulation of inventory records is the most common method of concealment. Inventory is altered either by changing the perpetual inventory or by false matching during the physical inventory.

***Mis-utilization of Information:*** An employee passes private and confidential information to an employee of another company to get some undue advantage. A software or design developed by a company is stolen by an employee of that company to transfer to a company where he can get a job based on that design or software.

***Misappropriation of Securities:*** The director of accounting and finance, who was responsible for making trades, left his computer unattended for a short time while signing into one of the company's investment accounts. Another employee, a senior accountant, took the opportunity to access the director's computer to sell 2 Crores worth of investments and have the proceeds mailed to the company. Due to lax internal controls, the employee was able to intercept the cheque and deposit it into her own bank account because this employee was in charge of reconciling the investment accounts.

## 4.3 Fraud through Manipulation of Financial Statements

Financial statement fraud or manipulation is a white-collar crime usually perpetrated by management insiders to represent a company in a more favorable fiscal light. It refers to the practice of using creative accounting tricks to make a company's financial statements reflect what the company wants its performance to look like rather than its actual performance. Fraudsters are motivated by personal gains, such as performance-based compensation; to enhance the company's reputation by misleading potential investors, or to simply buy time until financial mistakes and losses can be properly corrected.

Financial statement fraud is the deliberate misrepresentation of a company's financial statements, namely Balance Sheet, Income Statement and Cash Flow Statement, whether through omission or exaggeration, to create a more positive impression of the company's financial position, performance and cash flow. The manipulation invariably consists of either inflating revenues or deflating expenses or liabilities.

*Did you know?* Why Do Companies Manipulate Their Financial Statements?

The higher-paid executives who run major corporations can be tempted to "cook the books" on their financials for several potential reasons, such as:

- Feeling intense pressure to show a positive picture
- Tapering investors' expectations
- Triggering executive bonuses

*Caution*

Financial statement fraud is committed when people with access to financial documents and information manipulate data to make the company appear more successful.

The best way to prevent financial statement fraud is to have in place a system of strong internal controls that enforce the segregation of duties so that no single employee has the authorization to view and alter all financial data. This can be automated through an enterprise resource planning (ERP) system.

### Modus operandi of Financial Statements Manipulation

**Overstating revenue:** A company can commit fraud by claiming the money as received before the goods or services have been delivered. This can be done by prematurely recording future expected sales or uncertain sales. If the company overstates its revenue, it creates a false picture of fiscal health that may inflate its share price.

*Examples*

Billing to a customer with an intention of not shipping the goods and reversing the said sales in the ensuing financial year as sakes-return.

- Delaying entry of sales-return to increase revenue in the current financial year.

**Understating the Expense or Liability:** Understating expenses is a form of manipulating financial statements which are committed to increasing the revenue of the company. It results in an overstatement of assets or an understatement of liabilities.

*Examples*

A company fails to record accrued expenses to overstate the income and understate the liabilities.

- Shell companies are created with the sole motive to off-load liabilities from the principal company to the shell company's accounts.

**Inadequate Disclosure:** The information disclosed in financial statements must be accurate and clear so as not to mislead the reader. Accounting changes must be disclosed if they have a material impact on the financial statements. When this type of fraud is committed, items such as significant events, related-party transactions, contingent liabilities and accounting changes are obscured or omitted from the financial statements.

*Examples*

The following are examples of different types of transactions which amount to inadequate disclosures.

- False Book Entries in creating fictitious revenue
- Misapplication of funds raised through financial institutions.
- Mismatch of projections and deployment of Public funds through public issues
- Misclassification of heads of accounts in financial statements

**Overstating Assets:** This form of fraud occurs when a company overstates assets by failing to apply an appropriate depreciation schedule or valuation reserve, like inventory reserves. It will result in overstated net income and retained earnings, which inflates shareholders' equity. It also involves reporting Financial Assets at market price instead of their cost price. This is done to enhance a Balance Sheet so that ratios concerned with the assets of a company do not affect it.

*Examples*

- Inflated Inventory
- Enhanced amount of Accounts Receivables
- Creating Fictitious Assets

**Understating Assets**: This type of financial statement manipulation is common in public sector undertakings or government organizations as funds requirements are generated for the purchase of an asset as improper depreciation is charged to an asset.

**Concealment of liabilities or obligations:** Concealment is a type of fraud where liabilities or obligations are kept off the financial statements to inflate equity, assets and/or net earnings. Examples of concealed liabilities can include loans, warranties attached to sales and underreported health benefits, salaries and vacation time. The easiest way to conceal liabilities is to simply fail to record them.

**Timing differences:** This one involves understating revenue in one accounting period by creating a reserve that can be claimed in future, less robust periods. Other forms of this type of fraud are posting sales before they are made or before payment, reinvoicing past due accounts and prebilling for future sales.

**Transaction between Sister companies, Tax revenue, Losses and Siphoning off of funds with related persons**

**Fraud by large-sized companies with huge investments in Share Capital of Unlisted/Listed companies with no Trading**

## 4.4 Procedure-Related Fraud; Corporate espionage

Different types of frauds are committed by over-ruling or bypassing the procedures, carrying on business ultra vires the objects, fraudulently going into liquidation, siphoning off of funds and related-party transactions. Understanding what motivates employees to steal from companies is the key to detecting and preventing internal procedure-related fraud. Major procedure-related frauds are given below:

- Carrying business ultra vires the objects
- References to BIFR
- Fraudulently going into liquidation
- Merger & Amalgamation
- Siphoning off of FDI
- Transactions between sisters concerns
- Forex misuse

### Modus operandi of Procedural Lapses

Some of the methods adopted by the corporate sector for procedural lapses are:

**Public Issue Companies carrying on business ultra vires their Object Clause:** Large-sized public issue companies which mis-utilise the public money to continue to remain in business usually engage themselves fraudulently in pursuing objects which are not the main objects of the company and are in violation of the provisions of section 13(9) of the Companies Act, 2013. Such companies usually have Negative Net Worth but wait for an opportune time based on their large capital to attract gullible investors in to project ultra-virus objects.

**Frauds by the company with Foreign Direct Investments and Export Earnings**: The funds received through the Foreign Direct Investment route have to be seen with a critical eye. The origin of funds is important. Are the funds received from well-known parties from abroad, whether the funds are from a person of Indian Origin, whether the company is in profit or losses, and whether substantial monies have been invested by the Indian partner, will be the important parameters to determine whether such a company is prima facie likely to/ committing frauds?

The modus operandi of such companies is to incur large money in software development/technical know-how and pay very high salaries to their managerial and top personnel and grant huge loans

and advances, particularly to their sister concerns. Such companies either earn negligible profits or incur losses. Such companies also siphon/divert funds to such projects where foreign direct investment is banned. It may be relevant to mention that the export earnings companies which also have foreign direct investments are, in fact, Hawala operators and are not doing any productive work except to create illegal wealth.

**Companies engaged in investment in shares of Listed/ Unlisted Companies:** Certain companies belonging to a group engage themselves in investment in shares of other companies (belonging to their group). Such shares are purchased at par value. The funds of a flagship company are routed through the investor company for investment in the investee company. After a short time holding of these shares by the investor company, they are sold to individuals (who are directors/ relatives of directors of the investee company) at a rock bottom price of saying Re. 1/ per share against the original investment of 10/- per share. In the process, the valuable public funds of a flagship company are systematically siphoned off through the aforesaid investment route which finally hands up in the hands of a few individuals who maintain a controlling interest in such group companies. This fraud goes undetected as no disclosures in this regard are made by any professional who audits the account.

**Companies fraudulently going into Liquidation:** Companies who have either public stakes or financial stakes such as banks/financial institutions, after siphoning off of the funds of the companies try to take immunity and seek cover of this fraudulent activity by obtaining winding up fake order (usually getting winding up petitions filed by their own generated fake creditors). The motive of such companies is illegal.

**Reference to BIFR as a Sick Company**: Large public money/bank or financial institution money is systematically siphoned off when cases are referred to BIFR either for a rehabilitation package or/winding up of a company.

**Mala fide Merger and Amalgamation Schemes:** The merger and amalgamation schemes are prepared with the intention to defraud the creditors, and to avoid government dues. In some cases, the companies adopt the merger and amalgamation schemes with mala fide intentions with the purpose to conceal material information to defraud the creditors and approaching the jurisdictional High Court for merger and amalgamation, which can be termed procedural fraud.

## 4.5 Corporate Espionage

The term 'corporate espionage' has turned synonymous with 'industrial espionage. With the intensification of competition and the enlargement of profitability in business ventures, corporate officials began resorting to some innovative methods for obtaining information about their rivals. Industrial espionage refers to all the undercover activities that are performed by entrepreneurs for acquiring information about their business rivals for commercial gain. Targeted victims of espionage activities range from a rival business organisations to governmental agencies. Information can make the difference between success and failure, or profit and loss accounts in the business world. Theft or infringement upon the intellectual property or secret information of a company is the aim of corporate espionage.

Corporate espionage is a threat to any business whose livelihood depends on information. The information sought after could be a client list, supplier agreement, personal rewards, research documents, and prototype plans for a new product or service. As per the American Society for Industrial Security and Price Waterhouse Coopers, in 1999, 1000 companies lost more than $ 45 billion from the theft of trade secrets.

A company can become a victim of corporate espionage due to the following factors:

1. Social engineering;

2. Dumpster driving;

3. False pretenses;

4. Viruses and Trojan horses; and 5. Corporate identity theft.

Corporate espionage not only leads businesses to bankruptcy but also affects ties with friendly nations. Non-financial damages to business include public embarrassment for a company, tarnishing of the corporate image, loss of business confidence among partners or shareholders and a public misconception that the company is a security risk.

The various ways of Corporate Espionage are:

- Concealment of confidential information
- Infringement of intellectual property rights like trademark, copyright, patent and design.

**Modus operandi of Corporate Espionage**

The employees of the company or the company itself commit fraud by concealing the confidential information of the company for the benefit of its competitor company. The main modus operandi in such frauds is described below:

**(1) To conceal and act on confidential information: In such type of fraud, an employee of a company acts based on confidential information of his company.**

*Examples*

- Before the announcement of the information on the takeover, acquiring shares of that company to obtain a pecuniary advantage, speculating that he/she will be able to sell those shares in the takeover bid at a significantly higher price than the current market price.
- To pass on corporate information to a company that offered a job.
- To download trade secret files and then 'allegedly' shared files with other companies.

**(2) To use/infringe the trademark, copyright, patent or design of its competitor, to sell the product and to cheat the consumer:** The competitor similarly uses the trademark as of its competitor which results in a reduction of profits and a decrease in sales.

Thus, the effect of corporate espionage is almost wholly negative. This type of fraud can be prevented by keeping sensitive information secret and by putting a check on employees' behaviour.

## 4.6 Digital and e-commerce frauds

Digital fraud is when criminals try to use email, websites, malicious software or other methods to learn your personal details or trick you into paying them. Unfortunately, there are many types of digital fraud, and fraudsters don't discriminate. This means that you need to stay vigilant and educate yourself to avoid falling victim. The following outlines the most common types of digital fraud:

- **Phishing** activities aim to manipulate you into something that you normally wouldn't do, such as clicking on a link, opening an attachment, revealing personal information or transferring money. You may occasionally receive suspicious emails, SMS messages or phone calls claiming to come from CommBank that ask you to:
  Follow links and click through to fraudulent websites
  Update personal details
  Log on to NetBank via a link in an email

If you've received a phishing email and acted on the request, you may have been a victim. Message us in the CommBank app or contact us to report suspicious activity on your account. If you've received an email or text and haven't followed through on the instruction, email us a copy of the phishing email/SMS to hoax@cba.com.au

- **Malware** includes viruses, software, or attachments designed to target online banking on computers or mobile devices to redirect transactions without your knowledge
- **Porting** is the transfer of your mobile phone number from one service provider to another. Once the fraudster has access to your messages, they can retrieve one-time passwords and make payments via your online banking
- **Identity takeover** is the action of taking over your identity to access your current banking or create new bank accounts and loans. This usually involves obtaining a full name, date of birth, and address and passing identity verification over the phone to update NetBank login details.

In the digital age, online businesses are quickly becoming easy targets for cybercriminals. Scammers have a greater opportunity to create fake websites to disguise genuine online businesses or hack customer personal information if your eCommerce store doesn't take security measures.

Cash on delivery and prepaid orders are both vulnerable to e-commerce fraud. Today, e-commerce fraud takes many forms, as can be seen. Common e-commerce frauds include fake COD orders, fake delivery attempts, promo code misuse, and a variety of frauds such as inception, card validity testing, chargeback, and so on, just to name a few.

Purchase fraud or eCommerce fraud is illegal payment transactions that criminals or fraudsters make on a website without the account owner's knowledge, by using a False identity and Fake or stolen credit card.

Out of the many scams that hackers can use, there are 3 types of fraud that most eCommerce websites encounter:

Credit card fraud

Affiliate fraud

Phone fraud

## Modus Operandi of eCommerce fraud

### Credit card fraud

#### *Identity theft*

Identity fraud or identity theft occurs when fraudsters gain access to customer details by purchasing or hacking the user's account, and then implementing their phishing schemes. The stolen information and data include:

Personally identifiable information

Financial information

Passwords and security codes

Account takeover

*Caution*

This doesn't only affect the card owners but also the retailer as the buyers may request a refund. Also, it reduces the reputation of the seller because customers feel their personal and financial data on your eCommerce site is vulnerable.

#### *Chargeback fraud*

Chargeback fraud or friendly fraud takes place when the buyer keeps the online purchased items but still requests a refund for the following reasons:

Item wasn't received

The payment was made twice

The purchase was never made

#### *Clean fraud*

Clean fraud is much similar to legal payments made by legitimate customers because the impostor uses stolen credit card and cardholder information.

#### *Phishing*

Phishing is the practice of collecting the personal information of genuine users, including:

Credit card information

Card number

User ID and password

### Affiliate fraud

Violating the terms and conditions of an affiliate marketing program, affiliate fraud is the practice of manipulating registration and traffic statistics to generate commissions by either way:

Ask real customers to log into the merchant's online store with a fake account

Use a fully automated process

### Phone fraud

Telephone fraud or communication fraud is the use of telecommunications products or services to illegally obtain money from a customer's payment while not paying that amount to the telecommunication companies.

*Examples*

Extended warranty: Scammers know when your customers bought the car and the type of car to urge them to buy worthless services at a price.

"Free" trials: Scammers promise free trials but use the information to sign you up for one or more other products or services. You will have to pay monthly fees until you find out and cancel them.

## Summary

Corporate fraud consists of illegal, deceptive actions committed either by a company or an individual who is an employee of the company.

Corporate fraud commonly occurs for the same reason as any other fraud scheme – greed. However, amid the highly competitive global business environment of the modern world, it may also occur for other reasons. Many corporate fraud schemes consist of fraudulent accounting schemes used to make a company appear more profitable than it actually is. The impetus behind such schemes is the desire or perceived need to attract or retain investors.

Corporate fraud can be divided into five categories as shown below:

- Bribery and corruption;
- Misappropriation of assets;
- Fraud through manipulation of financial statements;
- Procedure-related fraud; corporate espionage;
- Digital and e-commerce frauds

Bribery and corruption are either in cash or in kind and include procurement fraud.

Asset misappropriation includes the misuse or theft of assets belonging to a company. Asset misappropriations can be divided between cash schemes and non-cash schemes. Misappropriation of assets affects investors and banks or financial institutions as it leads to manipulating the market valuation of securities for investors and stock for banks and financial institutions.

Financial statement fraud or manipulation is a white-collar crime usually perpetrated by management insiders to represent a company in a more favorable fiscal light.

Delinquent directors with the help of crooked professionals, tend to indulge themselves in a different type of fraud. Some companies with weak financial statements, to show a healthy financial position, manipulate the financial statements leading to a rosy picture of the company and the contravention of various provisions of the law go undetected.

Corporate espionage is due to the increase of competition in the global market place and this fraud can be caused by non-classification of sensitive information, absence of risk assessment to identify vulnerability, non-adoption of security policies and improper training to employees and users of the trade secrets, higher turnover and hoping culture which results in leakage of trade secrets and IPR secrets in the corporate world.

Purchase fraud or eCommerce fraud is illegal payment transactions that criminals or fraudsters make on a website without the account owner's knowledge, by using False identity, Fake or stolen credit card

Businesses are always at risk of interacting with individuals who intend to defraud or deprive the company of funds. While no company, even with robust internal controls, is entirely protected from fraud, there are several precautions that a business can implement to avert corporate fraud as best as possible. Avoid extending credit to the unknown, Evaluate risk, Implement and update privacy policies, Implement detection strategies, and Regularly complete bank statement reconciliations, Regular follow-up are a few precautions for reducing corporate fraud.

## Keywords

Bribery: It refers to the offering, giving, receiving, or soliciting anything of value to influence an 'official act', where 'official act' means the payments made to influence the decision of a government agent or employee.

Copyright: It is an exclusive right that is given to the creator of the original work. Earlier copyright law applied only to books, but now it covers a big range of work like dramatic work, music, paintings, sound recording, computer programmes, motion pictures, etc.

Cash larceny: It is the theft of funds after the transaction has been recorded.

Corruption: It is the dishonest or illegal behavior of powerful people. It can be categorized as bribery, economic extortion, illegal gratuity, and conflict of interest.

Design: It relates to the original shape of a manufactured article. It gives the owner the right to exclude others from making or importing articles with the particular design. A design is related to the configuration or surface decoration or both of an article.

Financial statement manipulation: It refers to the practice of using creative accounting tricks to make a company's financial statements reflect what the company wants its performance to look like rather than its actual performance.

Skimming: It is stealing the funds before they are recorded in the books of the company.

Trademark: It is a word, name, phrase, symbol or device that identifies and distinguishes the goods of one person from the goods of another person. The trademark is used to protect consumers as they can purchase the goods based on their prior knowledge, reputation or marketing. The trademark informs the consumers about the origination of goods or services.

## Self Assessment

1. _____ as any fraud undertaken by internal staff or external parties (with or without the help of an internal employee) against a company.

A. Employee Fraud
B. Corporate Fraud
C. E-Commerce Fraud
D. Corporate Espionage

2. In_____, a conspiracy develops between a vendor and an employee of the victim company.

A. kickback scheme
B. Bid-Rigging scheme
C. Skimming scheme
D. Larceny

3. _____ is a process in which several bidders conspire to split contracts up and ensure that each gets a certain amount of work.

A. kickback scheme
B. Bid-Rigging scheme
C. Skimming scheme
D. Bid pooling

4. Diverting the payments to fictitious employee accounts is an example of:

A. Asset misappropriation
B. Procedure lapse
C. Digital Fraud

D. Corporate espionage

5. Rita, a storekeeper at Amazon took out three cotton Kurtis for herself without intimating to her head or recording it in the store's ledger. Her act will be counted as:

A. eCommerce fraud
B. Asset misapplication
C. Asset misappropriation
D. Skimming

6. Identify the modus operandi of "Asset misappropriation" from the following:

A. Alteration in Inventory Records
B. Diverting Business to vendor
C. kickback
D. Fictitious suppliers

7. Identify the modus operandi of "Bribery and Corruption" from the following:

A. Fake sales
B. Alteration in Inventory records
C. Physical Padding
D. Over Invoicing

8. Misapplication of funds raised through financial institutions is an example of different types of transactions that amount to:

A. Bid Pooling
B. Corporate Espionage
C. Physical Padding
D. Inadequate disclosures

9. Inadequate disclosures is one of the modus operandi of:

A. Bribery and Corruption
B. Digital Fraud
C. Cooking the Books
D. Asset Misappropriation

10. Mr Hament was working in Frog textiles Limited. He gave an interview in Turtle textiles Limited (The biggest competitor of Frog textiles Limited). The interviewer asked Mr Hament to pass on Fron textiles Lit=mited internal information to get a job at a lucrative pay package. Mr Hament agreed to this and passed the asked information. Which kind of fraud, Mr Hament committed with Frog textiles Limited by doing this?

A. Asset Misappropriation
B. The window dressing of Financial statements
C. Corporate Espionage
D. Credit fraud

11. Identify the factors that make a company the victim of corporate espionage from the following:

A. Dumpster driving
B. Reference to BIFR as a sick company
C. Phishing
D. Inappropriate disclosures

12. Which of the following is not the reason behind making a company the victim of corporate espionage?
A. Social engineering
B. Corporate identity theft
C. Viruses and Trojan horses
D. Inventory misappropriation

13. Identify the procedural frauds from the following:
A. False pretenses
B. Social Engineering
C. Infringement of IPRs
D. Siphoning off of FDI

14. Which of the following is not a modus operandi of procedural fraud?
A. References to BIFR
B. Trademark infringement
C. Forex misuse
D. Transactions between sister concerns

15. Mehta and Sons overstated the closing inventory to increase the income from the sale of inventory as the cost of goods sold is reduced for those inventories which have been sold. This amounts to:
A. eCommerce fraud
B. Financial Statement fraud
C. Procedure-related fraud
D. Bribery

## Answers for Self Assessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | B | 2. | A | 3. | D | 4. | A | 5. | C |
| 6. | A | 7. | D | 8. | D | 9. | C | 10. | C |
| 11. | A | 12. | D | 13. | D | 14. | B | 15. | B |

## Review Questions

1. Explain the modus operandi of Bribery and Corruption.
2. What do you mean by misappropriation of assets. How do the employees manipulate assets? Explain.
3. What is financial statements fraud? Explain the forms of financial statement fraud.
4. Illustrate the methods adopted by the companies, leading to financial statement fraud.
5. Examine the role of inadequate disclosures in committing financial statement fraud.
6. Explain the methods adopted by the corporate sector for procedural lapses.
7. Explain the types of frauds that are committed by overruling the procedures.

8. What is corporate espionage? Evaluate its role in committing corporate fraud.
9. Explain digital and eCommerce frauds.
10. How do fraudsters commit eCommerce fraud. Explain.
11. Write short notes on the following:

A. Kickback
B. Over invoicing
C. Bid-Rigging schemes
D. Digital fraud

## Further Readings


- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2009). *Forensic Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.
- Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.
- Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). *Forensic Accounting and Fraud Investigation* (CPE ed.). John Wiley & Sons.


### Web Links

- https://www.netsuite.com/portal/resource/articles/accounting/financial-statement-fraud.shtml#:~:text=Financial%20statement%20fraud%20is%20the,position%2C%20performance%20and%20cash%20flow.
- https://corporatefinanceinstitute.com/resources/knowledge/accounting/financial-statement-manipulation/
- https://azraelfranz.com/news/7-ways-to-avoid-corporate-fraud/
- https://www.magestore.com/blog/types-of-ecommerce-fraud-and-how-to-prevent-them/#:~:text=for%20online%20frauds-,What%20is%20eCommerce%20fraud%3F,Fake%20or%20stolen%20credit%20card
- https://www.blackhawkintelligence.com/investigative-services/financial-fraud-investigations/common-questions-corporate-fraud/

# Unit 05: Corporate frauds in India

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the features of Corporate fraud in India.
- examine the various Corporate Frauds in the Indian Banking sector.
- identify the reasons forthe increase in Bank Scams in India.
- review the steps that need consideration for a reduction in the number of Bank Scams in India.
- examine the mechanism and consequences of infamous corporate fraud cases in Indian Capital markets.

## Introduction

Prime Minister Narendra Modi promised to make the Indian economy a $5 trillion economy, but instead, in just over seven years, bank fraud has surpassed $5 trillion. It's worth noting that India's total fraud loans in 2020-21 alone amount to Rs 1.37 lakh crore, accounting for 99 percent of all bank frauds.According to the Reserve Bank of India (RBI) data acquired under the Right to Information (RTI) Act, banks operating in India accounted for fraud of Rs 4.92 trillion as of March 31, 2021, accounting for over 4.5 percent of total bank credit. 90 banks and financial institutions reported a total of 45,613 occurrences of loan theft, according to the data.

The State Bank of India (SBI), ICICI Bank, and HDFC Bank had the most incidences of over 50,000 frauds that affected Indian institutions in the recent 11 fiscal years. Several international banks with operations in India have also reported scam cases totalling billions of rupees over the same period.There are news reports every few weeks of some bank scam which is breaking the trust of the common man in the banking system.

It includes the ABG Shipyard, Nirav Modi and Mehul Choksi scam involving the Punjab National Bank, the case of businessman Vijay Mallya, the Andhra Bank fraud, the Kanishk Gold Bank fraud, the IDBI Bank fraud, etc. The present unit discusses the major corporate fraud in India keeping in consideration the relevance of them to educate students about banking and other corporate frauds that make a large number of persons as victims of fraud.

## 5.1 Features of Corporate Frauds in India

Based on different frauds that occurred in the corporate sector during the last 20 years, the following features of corporate fraud can be drawn:

### Fraud Perpetrators

A careful look at the major scams in the corporate world in India and abroad reveals that the maximum number of frauds has been perpetrated either by the company management or by its top executives. The management or the executives, in connivance with the unscrupulous professionals and consultants, committed fraud through various modus operandi to make personal gains at the cost of other stakeholders. This may be partly due to the non-existence of independent directors and members in the audit committees.

### Common types of Frauds

It is noted that the most prevalent type of fraud in India and abroad is the manipulation of financial statements to evade taxes and other government levies. The second largest type of fraud prevailing in the corporate world is the one resulting from procedural lapses. These procedures include the carrying on of business ultra vires the company objects, merger and amalgamation, and seeking company liquidation on grounds having mala fide intentions.

### Lack of Action against Perpetrators

Companies are reluctant to take legal recourse against employees responsible for committing fraud. A few companies take disciplinary action against unscrupulous employees and their associate professionals. This may be due to fear of damages to the company's goodwill and reputation if news about the fraudulent incident leaks into the public domain. Also, companies prefer to avoid reporting any economic offence to a regulator. Companies are generally interested in recovering the defrauded money rather than getting the culprit punished. The analysis of cases of corporate fraud reveals that the fraud perpetrators got imprisonment for a period ranging from one year to 22 years, besides imposition of penalty.

### Accountability

In the first reported major case of corporate fraud, namely, the Hari Das Mundhra case, the then Union Minister of Finance, the legendary T.T. Krishnamachary, and the Finance Secretary both had to resign from their posts. No such action was ever taken in any subsequent case. But, then that was the era of Jawaharlal Nehru and Lal Bahadur Shastri. In fact, no senior functionary in the government either owned up to the responsibility these days.

### Insufficient Authorities

The lack of an effective regulatory and compliance mechanism and weak law enforcement are equally responsible for facilitating fraud. Corporate frauds were unearthed because of legislation such as the Right to Information Act (RIT) and Public Interest Litigation (PIL).

### Insufficient Powers with Fraud Regulating Agencies

It is noted from the above cases that after the introduction of the SEBI Act in 1992, corporate frauds have been rampant in India, which may probably be because SEBI does not enjoy the powers of a criminal court. Moreover, the SEBI also suffers from jurisdictional disadvantages in respect of non-listed companies. It appears that the major regulator of the corporate world has not made its presence felt in the market insofar as the regulation of corporate frauds is concerned.

### Approach of the Adjudicating Agencies

The corporate fraud perpetrators have been treated in courts at par with other fraudsters, while the causes and consequences are entirely different and far-reaching. The time lag in judicial decisions is also responsible for inducing corporate fraud as no separate wing has existed to punish the guilty expeditiously.

### Time Taken in Disposal of Cases

The disposal of the fraud cases has taken a relatively long period on average. Most of the cases took more than 7 years. The minimum time was taken in the Satyam Case, where the main accused B. Ramalinga Raju, the company chairman, was convicted in two months as he himself confessed to the crime. Companies hesitate to record such matters to the police, apprehending the hardship they may face during the investigation and prolonged judicial trials.

### Weak Anti-fraud Measures

Companies still rely on old traditional techniques and measures for protection against fraud. Reliance on Internal and External Audit and codes of conduct are the main measures to detect and prevent frauds. These methods are not sufficient for detecting and preventing frauds. A few companies have proactive fraud risk management initiatives and whistle-blowing mechanisms. It is surprising as fraudsters are using advanced tools and technology to perpetrate frauds.

## 5.2 Infamous Corporate frauds in Indian Banking & Insurance Sector

### 11 Biggest Corporate Frauds in Indian Banking Sector in the Last Decade

Vijay Mallya Fraud Case (2016)

Punjab National Bank Scam (2018)

Winsome Diamond Scam (2016)

ABG Shipyard Fraud Case (2022)

Kanishk Gold Bank Fraud (2017)

Andhra Bank Fraud (2017)

Rotomac Pen Scam (2015)

Videocon Case (2019)

R.P. Info Systems Bank Scam (2018)

IDBI Bank Fraud (2018)

DHFL Scam

Notes

### 1. Vijay Mallya Fraud Case (2016)

Businessman Vijay Mallya's bankrupt Kingfisher Airlines owes more than Rs 10,000 crore to more than a dozen banks. He fled India on March 2, 2016, the same day that some public-sector banks filed a petition against him with the Debt Recovery Tribunal.

The "King of Good Times" and his businesses have been steeped in financial scandals and controversies for a long time. Kingfisher Airlines, which began operations in 2005, was forced to cease operations in 2012 due to increasing liabilities.

A group of 17 Indian banks is trying to collect roughly Rs 10,000 crore in loans that Mallya is accused of using to gain shares in more than 40 companies around the world. The largest lender was SBI, which had 1600 crores, followed by the Punjab National Bank, which had 800 crores, IDBI, which had 650 crores, and the Bank of Baroda, which had 550 crores.

A court under the Prevention of Money Laundering Act (PMLA) named Mallya a repetitive offender in June 2016. He was arrested in April 2017 on an extradition warrant by Scotland Yard, although he is now out on bail. The Fugitive Economic Offenders Act designated him a fugitive economic offender in January 2019. The government is endeavouring to extradite Mallya from the United Kingdom.

### 2. Punjab National Bank Scam (2018)

Punjab National Bank had informed of Rs 11,400 crore scam in 2018. The theft was dubbed the biggest in Indian banking history at the time. Jeweller Nirav Modi, Mehul Choksi, Nishant Modi, Ami Modi and others, including some PNB staff, were the main defaulters identified.

'Letters of undertaking' (Lous) were fraudulently issued by a junior official at PNB, to get short-term loans from overseas bank branches to pay the sellers. As a result, the transactions were never logged in the bank's main system, and the fraud went unnoticed by PNB's higher management.

The Nirav Modi and Gitanjali companies defrauded 30 Indian banks' international branches for a total of Rs 11,400 crore. The fraud was exposed after the CBI investigation. Modi left India just days before the fraud became public.

The Indian government accused him of criminal conspiracy, cheating, money laundering, corruption, criminal breach of trust, fraud and breach of contract in the PNB case in August 2018. Modi is presently detained in Wandsworth Prison in London's southwest.

### 3. Winsome Diamond Scam (2016)

After Kingfisher Airlines and Punjab National Bank defaulter Nirav Modi, Mehta's Winsome is India's third-largest corporate defaulter. Jatin Mehta, the promoter of Winsome Diamonds &Jewellery, is a Gujarat-based diamond trader. He owes a group of banks more than Rs. 6,500 crore.

Jatin Mehta's Winsome Diamonds fraudulently acquired letters of undertaking from Indian banks. It should be mentioned that the faults were caught for the first time in 2014. The group has been deemed a willful defaulter by banks since mid-2013 when it failed to repay its loans. The overall debt is estimated to be around Rs 7,000 crore.

More than ten cases have been filed against the businessman by the CBI. It filed charges against 21 persons, including Mehta and his wife Sonia, in 2018. Two former Canara Bank CEOs and 15 government employees were also charged with assisting Mehta in getting the loan. In addition, the CBI instructed Interpol to issue a Red Corner Notice against Mehta in a letter.

The family managed to flee the proceedings without leaving a trace. Jatin Mehta relocated to Montenegro, a Balkan country in South-East Europe, with his family. According to the investigating officer, the Mehta family developed their business in different countries after fleeing India.

### 4. ABG Shipyard Fraud Case (2022)

In its Second biggest bank fraud case, the CBI has booked ABG Shipyard Ltd and its former chairman and managing director Rishi Kamlesh Agarwal along with others for allegedly cheating a consortium of banks led by State Bank of India of over Rs 22,842 crore.

ABG Shipyard was incorporated on 15 March 1985 and has since been one of the big players in India's shipbuilding and repair business. Their shipyards are located in Dahej and Surat in Gujarat.The company is known for creating newsprint carriers, self-discharging and loading bulk cement carriers, floating cranes, interceptor boats, dynamic positioning diving support vessels, pusher tugs and flotillas for leading companies in India and abroad.

#### *How Much Money Does ABG Shipyard Owe To Banks?*

| Bank | Amount (In INR Crores) |
|---|---|
| ICICI Bank | 7,089 |
| SBI | 2,925 |
| IDBI Bank | 3,639 |
| Bank of Baroda | 1,614 |
| Punjab National Bank | 1,244 |
| Exim Bank | 1,327 |
| Indian Overseas Bank | 1,244 |
| Bank of India | 719 |

Caution:

Apart from the above, ABGSL also owes small amounts to other banks.

#### *What is this Scam all about?*

The company reportedly took a big hit from the financial crash of 2007-08 and by 2012, its coffers were drained. The crash led to the company taking massive loans from several banks.

However, it diverted this cash to its overseas subsidiaries and even transferred money to several offshore parties. This alleged fraud, according to a probe conducted by E&Y in January 2019, took place between April 2012 and July 2017.

At the crux of the scam is a web of transactions made by the shipping firm. The money loaned by ABG Shipyard, according to the FIR, was used to repay loans and pay for expenses of ABG Group

of Companies and for letters of credit. This money was used to purchase properties being linked from funds provided by ABG Shipyard.

"After reviewing annual reports of ABG SL for the financial year 2014-15 and ledgers it appears that ABG SL had paid accommodation deposits worth Rs 83 crores in total to companies like Aries Management Services, GC Properties, Gold Croft Properties, before review period (in 2007-08). And these parties were potentially related to ABG SL and its promoters," as per FIR.

ABGSL, which turned into a non-performing asset (NPA) in 2013, also violated the terms of Corporate Debt Restructuring (CDR). CDR is a mechanism in which the lender banks either reduce the interest rates on the loans of the distressed borrower company or increase the tenure of the repayment.

The defendants are accused of embezzling Rs 22,842 crore from SBI and 27 other banks and lenders. The CBI has arrested several people in connection with the ABG Shipyard case investigation.

 Task

Identify the fraudsters and victims of the following scams and explain the mechanism of the scams as well:

a) Andhra Bank Fraud (2017)

b) Rotomac Pen Scam (2015)

c) Videocon Case (2019)

d) R.P. Info Systems Bank Scam (2018)

e) Kanishk Gold Bank Fraud (2017)

### 5. Videocon Case (2019)

The CBI filed an FIR in 2019 against former ICICI Bank CEO Chanda Kochhar, her husband Deepak Kochhar, and Videocon group MD Venugopal Dhoot, alleging irregularities in loans granted to the group by the bank in 2012.

In this loan case, a panel led by Justice BN Srikrishna found Kochhar had broken the bank's code of conduct. When Kochhar was the CEO of ICICI Bank, the bank loaned Rs 3,250 crore to Venugopal Dhoot's Videocon Group.

In 2016, a shareholder whistleblower named Arvind Gupta, who owns shares in both ICICI Bank and Videocon Group, claimed that Kochhar influenced a Rs 3,250-crore loan to Videocon Group in 2012 in exchange for a deal in NuPower Renewables and Supreme Energy, a clean-energy firm managed by her husband. Another whistleblower filed a complaint against the bank and its top management in 2018.

The CBI opened an investigation the same year and questioned Deepak Kochhar and his brother Rajiv Kochhar. Between 2009 and 2011, the ICICI Bank approved loans worth Rs 1,875 crore to the Videocon Group and its subsidiaries. Dhoot's Supreme Energy issued a Rs 64 crore loan to NuPower Renewables, in whom Deepak Kochhar owns a 50% stake, just months after the loans were approved.

### 6. DHFL Scam (2022)

The Indian banking system, which is struggling with the issue of mounting bad loans, has been hit by another banking fraud case. This time the Central Bureau of Investigation (CBI) has booked promoters of the non-banking finance company "Dewan Housing Finance Limited (DHFL)" of defrauding a consortium of 17 banks worth Rs 34,000 crore. DHFL banking fraud is being termed as the country's biggest scam in the banking industry after ABG Shipyard's fraud case of Rs 20,000 crore which was reported earlier this year.

#### *Issue*

Recently, Dewan Housing Finance Corporation Limited (DHFL) has deceived a consortium of banks driven by the Union Bank of India to the tune of Rs. 35,000 crore through financial misrepresentation.

The case has been registered on a complaint from the Union Bank of India (UBI). According to the UBI complaint, since 2010, the DHFL has extended credit facilities of over Rs 42,000 crore by the consortium of which Rs 34,615 crore remain outstanding. The loan was declared NPA in 2019 and fraud in 2020.

The Union Bank of India in its complaint has alleged that DHFL had taken Rs 42,871 crore as loans from a consortium of 17 banks between 2010 and 2018.

It said the company started defaulting in loan payments from 2019.

The bank alleged that the promoters along with others siphoned off and misappropriated a significant portion of the funds by falsifying the books of DHFL and dishonestly defaulted on repayment of the legitimate dues of the said consortium banks.

This caused a loss of Rs 34,615 crore to the 17 banks in the consortium.

### *When And How Was The Scam Unearthed?*

Earlier in 2019, Investigative platform Cobrapost alleged the primary promoters of DHFL and their associate companies had committed a "systemic fraud" to siphon off public money.

Cobrapost alleged that the "scam" was committed by giving out funds in secured and unsecured loans to "dubious" shell or pass-through entities, purportedly related to DHFL's own primary stakeholders through their proxies and associates. The funds, as alleged, were re-routed to the firms allegedly controlled by them.

Responding to the charges, DHFL issued a statement saying: "This mischievous misadventure by Cobrapost appears to have been done with a mala fide intent to cause damage to the goodwill and reputation of DHFL and resulting in erosion in shareholder value.DHFL received an email at 8.44 a.m., with a follow-up reminder one hour later, seeking answers to 64 questions from Cobrapost, many of which were laced with political innuendos."

Following this, the lender banks in February 2019 appointed KPMG to conduct a "special review audit" of DHFL from April 1, 2015, to December 31, 2018.

### *What Did The KPMG Audit Reveal?*

KPMG found a diversion of funds in the guise of loans and advances to related and interconnected entities and individuals of DHFL and its directors.

A forensic audit conducted by the KPMG observed that "large amounts were disbursed as loans & advances by the borrower company to a number of interconnected entities and individuals with commonalities to DHFL Promoter Entities, which were used for the purchase of shares/debentures."

### *Where Was The Money Disbursed?*

The account books showed that 66 entities having commonalities with DHFL promoters were disbursed Rs 29,100 crore against which Rs 29,849 crore remained outstanding. Another major outstanding in DHFL accounts was Rs 11,909 croredue to loans and advances worth Rs 24,595 crore given to 65 entities. DHFL and its promoters also disbursed Rs 14,000 crore as project finance but showed the same as retail loans in their books.

### *Summary of the case*

In 2019, a consortium of banks had held a meeting to take cognizance of the serious allegations of loan repayment default against the DHFL.A core committee of 7 of the largest banks — the State Bank of India, the Bank of Baroda, the Bank of India, Canara Bank, the Central Bank of India, Syndicate Bank and the Union Bank of India was formed.The Central Bureau of Investigation in its first information report, has shown that the SBI was the most badly hit.

Essentially, the Bank of India and Canara Bank have been plundered to the tune of more than Rs. 4,000 crore each by the DHFL.Also, more than Rs. 3,000 crore each has been supposedly cleaned up by the DHFL from the Union Bank of India and the Punjab National Bank.

## 5.3 Infamous Corporate frauds in Indian Capital Market

### The Harshad Mehta Case (1992)

Born in a modest Gujarati Jain family, Harshad Mehta was a stockbroker and is reported to have engineered the rise in the Bombay Stock Exchange in the year 1992. Starting as a dispatch clerk in the New India Assurance Company Ltd, he along with his brother, Ashwin developed an interest in the stock markets operations. His earlier childhood was spent in Mumbai (Kandivali), where his father was a small-time businessman. Later, the family moved to Raipur in Chhattisgarh.

Harshad Mehta started his venture, by establishing a company known as Grow More Research and Asset Management Company Limited. Mehta gradually rose to become a stock broker on the Bombay Stock Exchange and developed an expensive lifestyle. He lived in a 15,000 square feet (1,400 square metre) apartment, which had a swimming pool as well as a golf patch. He rose and survived the bear runs. This earned him the nickname of the Big Bull of the trading floor. By the late 1980s, the media started projecting him as a 'stock market success' and 'the story of rags-to-riches'. By 1990, Mehta had risen to prominence in the stock market. He was buying shares heavily, the shares which attracted his attention were shares of Associated Cement Company Limited (ACC). He took the price of ACC shares from 200 to 9,000 per share.

In April 1992, the Indian stock market crashed, and Harshad Mehta, the person who was all along considered as the architect of the Bull Run was blamed for the crash. He had manipulated the Indian Banking systems to siphon off the funds from the banking system, and used the liquidity to build large positions in a select group of stocks. The broker was dipping illegally into the banking system to finance his buying. The crucial mechanism through which the scam was affected was the ready-forward (RF) deal and the bank receipt (BR). The RF is an evidence of a secured short-term loan from one bank to another. Mehta used the RF deal with great success to channel money through the bank. A typical RF deal involves two banks brought together by a broker instead of a commission. The broker handled neither cash nor securities. In this settlement process, the delivery of securities and payments was made through the broker. That is, the seller handed over the security to the broker, who passed them to the buyer, while the buyer gave the cheque to the broker, who then made the payment to the seller. In this settlement process, the buyer and the seller might not even know whom they had traded with, rather being known only to the broker. This the brokers could manage primarily because by now they had become market-makers and had started trading on their accounts. To keep up a semblance of legality, they pretended to be undertaking the transactions on behalf of a bank.

Another instrument used in a big way was the bank receipt (BR). Securities were not traded in reality in a ready-forward deal but the seller gave a BR which was a confirmation of the sale of securities. It acted as a receipt for the money received by the selling bank. It promised to deliver the securities to the buyer. It also stated that the seller holds the securities for the time being in the trust of the buyers. To figure this out, Mehta needed banks which could issue fake BRs (i.e., BRs not backed by any government securities). Two small and little-known banks, the Bank of Karad and the Metropolitan Co-operative Bank, came in handy for this purpose. These banks were willing to issue BRs as and when required for a fee. Once these fake BRs were issued, they were passed on to the other banks which, in turn, gave money to Mehta, obviously assuming that they were lending against government securities, whereas this was not the case.

This money was used to drive up the stock prices in the stock markets. At the time of returning the money, the shares were sold for a profit and the BR was retired. The game went on as the stock prices kept going up, and no one had a clue about Mehta's modus operandi. Once the scam was exposed, many were left holding the BRs which did not have any value; the banking systems had been swindled of a whooping 4,000 crore. The concept of BR was finally removed and many people were bankrupted and committed suicide.

Harshad and his associates by taking advantage of the loopholes in the banking system, triggered a securities scam that diverted funds to the tune of 4,000 crore ( 40 billion) from the banks to stockbrokers from April 1991 to May 1992. He was later charged with 72 criminal offences. A special court also sentenced Sudhir Mehta, Harshad Mehta's brother, and six others, including four bank officials, to rigorous imprisonment (RI), ranging from 1 year to 10 years, on the charge of duping the State Bank of India to the tune of 600 crore ( 6 billion) in connection with the securities scam that rocked the financial markets in 1992. He died in 2002, leaving behind many court cases pending against him.

In 2006, a Hindi movie known as 'Gafla' was released, the movie was about a stock market scam and was based on the Big Bull of the stock market 'Harshad Mehta'. The movie showed a lot of instances from his life. This movie won the best award at Cyprus Film Festival in 2008.

## The CR Bhansali Case (1992-96)

CR Bhansali, a Chartered Accountant, started his financial consultancy business in the name of a proprietorship firm, CRB Consultancy in Calcutta. He provided management issue services to well-known companies. Later, he acquired a Company Secretaryship qualification, a PhD degree, a Membership of the Massachusetts Interiocal Insurance Association (MIIA) of US and a diploma in journalism. He joined as Registrar of Companies, Delhi, but had to leave on being caught in short-changing the Registrar's client.

He formed CRB Consultants Private Limited and then changed this name as CRB Capital Market Private Limited and later converted it into a public limited company. The company provided services of Merchant Banking, Leasing and Hire Purchase, Fixed Deposit and Resource Mobilisation, etc. It got a card of the Bombay Stock Exchange as well as National Stock Exchange. He first established a finance company, CRB Capital Markets, followed by CRB Mutual Fund and CRB Share Custodial Services Limited CRB Corporation Limited, an another CRB company, raised 84 crore through three public issues, between 1993 and 1995. CRB Share Custodial Services Ltd. raised 100 crore in 1995. Bhansali launched CRB Mutual Funds which raised 230 crore from the market. Another 180 crore was raised from the investors through fixed deposits. CRB Capital Markets raised a whopping 176 crore in three years. CRB Mutual Funds raised 230 crore out of which 180 crore was received as fixed deposits. Bhansali also succeeded in raising about 900 crore from the market. He borrowed more money from the market, which led to a grave financial crisis.

He was an expert to sell investment companies formed by him. He widen his network with the officials of the Registrar of Companies, and the Controller of Capital Issues. He got listed their companies by raising money through maiden public issues and then transferred their companies to the buyer who needed such companies. Bhansali used his private company to rig share prices in order to raise money from the market. Through his private company, he bought his own stock and then used his Public Limited Company to buy into each other as crores holding. Within a period of four years, from 1991 to 1995, Bhansali's empire flourished with the total income from 1.2 crore to 103 crore. The thrust areas of leasing and hire-purchase shot up from a paltry 2 lakh, in 1991, to as much as 16 crore, in September 1994.

CRB opened a current account with the Securities and Exchange Board of India for payment of interest, dividend, redemption, cheque and then payment warranty could be honoured by any branch but was required to deposit the upfront amount in his current account together with the list of payments. The SEBI branches honoured all the dividend warrants without checking with headquarter but later on the SEBI realised that he had withdrawn few crores of rupees due to lack of communication and co-ordination between the banks and their branches. He cheated various banks to the tune of 1,200 crore.

CRB defrauded the investors and the regulatory authorities. Approximately 400 complaints from depositors were there against CRB companies. The CRB could not repay his liabilities and the CBI locked and sealed its group offices and arrested the company directors and froze the bank account of group companies.

CRB Caps' net worth went up from 2 crore in 1992 upto 430 crore in 1996. In the mid-1996, various frauds were committed by CRB. An FIR was filed against CRB under Section 120B, read with Section 420, of the IPC, and Section 13(2), read with 13(1) D of the Prevention of Corruption Act. Bhansali was charged with fraud, cheating and siphoning off of funds from the SEBI. He was imprisoned for 7 years.

## The UTI Case (2000)

The Unit Trust of India (UTI) was established through an Act of Parliament in 1964, as a mutual fund organization to channelize the public savings giving a guaranteed return to the investor. Among 87 schemes of UTI, the US-64 was the most popular one, giving the highest return and having 2 crore investors, the bulk of whom were small savers, retired people, widows, and pensioners. By February 2001, the UTI was managing funds worth 364,250 crore through over 92 saving schemes, including the US-64, Unit Linked Insurance Plan, and the Monthly Income Plan etc. UTI's distribution network was well spread out, with 54 branch offices, 295 district representatives and about 75,000 agents across the country.

The Chairman of UTI, using arbitrary powers, decided to invest a huge amount of 40 crore and substantial amount of UTI funds were invested in the infamous 'K-10 list' of Keten Parekh stock. The UTI continued to buy these shares even when their market value began to crash in order to pop up the share values of these stocks. The trust saw its 30,000 portfolio (value of stocks) lose half of its value within a year. In order to bail-out the UTI, the BJP-led NDA government provided a large amount of 3,500 crore.

Further, the UTI bought 34 crores worth of shares in Cyberspace Infosys Ltd at a huge price of 930 per share. The UTI also invested in junk bonds, including Pritish Nandy Communications ( 1.5 crore), Jain Studios ( 5 crore), and Sanjay Khan's Numero Uno International ( 7.5 crore). This amounted to nothing but handing over people's money (investments) to the rich and powerful people. Thousands of crores of rupees were siphoned off to big business houses and prominent individuals, including the UTI chairman and some bureaucrats and politicians.

The Chairman engaged in a high profile propaganda compaign to promote UTI (spending crores of rupees on the top advertising company, Rediffusion), while at the same time leaking information to the big companies to withdraw their funds. The Chairman duped the millions of small investors through false propaganda and allowing profits to big companies which had invested in the UTI. P.S. Subramanyam, former UTI Chairman, M. Kapur and S.K. Basu, executive directors of UTI Bank, and Rakesh G Mehta, stockbroker, were charged by the Central Bureau of Investigation (CBI) for their involvement in the scam. According to the CBI, 40,000 shares of Cyberspace, at the rate of 830/- per share, were purchased by the UTI, for a sum of 3.33 crore, from Rakesh Mehta, when there were no buyers for these shares. The conspiracy caused a loss of 32 crore. P.S. Subramanyam, M. Kapur, S.K. Basu, Rakesh Mehta and Arvind Johri 'promoter of Cyberspace', were arrested and imprisoned for three years each. However these person claimed that the said investment of 40,000 shares were made on the advice of the equity research cell of UTI.

During the two months prior to the freezing of dealings in the UTI shares, a huge sum of 4,141 crore was redeemed. Of this, 4,000 crore (97 per cent) were corporate investments. What is more surprising, they were re-purchased at the price of 14.20 per share (face value of 10) when its actual value (NAV-net asset value) was not more than 8. As a result, the UTI's small investors lost a further 1,300 crore to the big corporate. The huge withdrawals further precipated the crisis.

Simultaneously, it declared a pathetic dividend of 7 percent (10 percent on face value), which is even lower than the rates of interest given by the banks and post offices on savings schemes. Such freezing of legally-held shares is unheard of and is like overnight declaring 100 notes as invalid for some time. Thus, the two crore shareholders could not re-invest their money elsewhere and had to passively see their share price erode from 14 (at which they would have purchased it) to 8 and get interest at a mere 7 percent on their initial investments. Fearing a back-lash, the government/and the UTI announced the ability to re-purchase UTI shares at 10, i.e. at 30 percent below the purchase price. The UTI Chairman got imprisonment of 3 years.

## The Ketan Parekh Case (2001)

Ketan Parekh (KP), a Chartered Accountant, followed into Harshad Mehta's footsteps to swindle crores of rupees from the banks and had bigger plans in mind. Known as the 'Bombay Bull', and a Chartered Accountant by profession, he was managing his family business, NH securities formed by his father. He had connections with movie stars, politicians and international entrepreneurs. Ketan Parekh developed network of companies involved in stock market operations and held stakes in Amitabh Bachchan Company Ltd., Mukta Arts, HFCL, Zee Telefilms, Penta Media Graphics, Pritish Nandy Corporation, Himachal Futuristics, Global Tele-Systems, Satyam Computers, DSQ Software, etc.

Ketan Parekh selected these companies for investment which was listed high-growth company with low capital base. He took advantage of low liquidity in these stocks and these companies were known as 'K-10' stocks. He did not have enough money to buy large stocks and brought shares when they were trading at low prices and traded in these shares and saw the prices go up and when the prices was high, pledged these shares with the banks as collateral security. When the price was so high, he pledged the shares with banks as collateral for funds. His modus operandi was to raise funds by offering shares as collateral security to the banks. The share prices were rising, but it reversed when the markets started crashing in March, 2000. KP was asked to either pledge more shares as collateral or return some of the borrowed money.

By April 2000, mutual funds substantially reduced their exposure in the 'K-10 stocks'. By December, 2000, Ketan Parekh began to face liquidity problems and lost a lot of money. Because of the liquidity problem, Ketan Parekh was finding it extremely difficult to push the prices of stocks upward. Taking the advantage of this situation, the International bear cartel got together and started selling "KP Stocks" in the hope of buying them at a cheap rate at a later stage. Brokers of BSE provided sensitive information to the bear cartel about the market exposure of Parekh. The sudden selling of shares created a panic situation in the markets. Ketan borrowed 250 crore from Global Trust Bank to fuel his ambition. According to the RBI regulations, a broker is allowed a loan of only 150 crore ( 15 million). He along with his associates also managed to get 1,000 crore from the Madhavpura Mercantile Co-operative Bank. Even the Madhavpura Bank started off-loading the shares it was holding as collateral from Parekh, fearing his inability to pay back the borrowed funds. All these factors further contributed the steep decline of the prices of the KP Stocks. The SEBI launched an immediate investigation into the volatility of stock markets. He was charged with defrauding the Bank of India of about $30 million among others.

This scam created a historical impact on the financial status of the Bombay Stock Exchange and also on the faith of investors in its working. It was a case of nexus between the brokers, promoters and the bankers. The SEBI was accused of its reactive approach rather than proactive approach. Its overlooked the unusual price movement and tremendous volatility in certain shares. The huge erosion of amount could be avoided if the SEBI had shown its alertness. Ketan Parekh arrest was also not due to the SEBI's timely action but the result of complaints by the Bank of India. The SEBI started implementing several measures to control the damage. A historical decision to ban the 'badla' system in the country was taken. effective from July, 2001 and a rolling settlement system for the 200 Group-A shares was introduced on the BSE. Ketan Parekh is an example of the root that was within the Indian financial and regulatory systems and if the regulatory authorities had been alert, the huge loss could have been avoided. Ketan Parekh got an imprisonment of one year.

## The IPO Demat Case (2005)

The YES Bank entered into the Indian capital market by Initial Public Offerings (IPOs) in 2005. Roopalben Panchal allegedly opened numerous fictitious demat accounts to obtain the shares of the YES Bank and other companies and raised finance on the shares allotted to her. In 2005, the Securities and Exchange Board of India (SEBI) detected irregularities in the buying of YES Bank shares; and conducted an investigation into the IPO allotments. It was found that Roopalben Panchal was controlling about 15000 fictitious demat accounts. The SEBI noted that the fictitious investors through their fake accounts obtained the shares and transferred them to financers, who, in turn, sold these shares on the first day of listing to earn huge profits between the IPO price and the listing price.

The SEBI conducted investigation of the IPO's of the companies which brought their shares during the period of 2003 to 2005. The major IPO's which were investigated by the SEBI included Jet Airways, Sasken Communications, Suzlon Energy, Punj Lloyds, JP Hydro Power, IDFC, NTPC, PVR Cinema and Shringar Cinema. Similar irregularities were found by the SEBI in the IPO's of these companies. The investigation of the SEBI identified more operators and market intermediaries involved in the misuse of the IPO's during 2004-2005. In another case, the SEBI found that Jayesh P. Khandwala, along with the proprietor of Zealous Trading Company, opened thousands of fictitious demat accounts to corner the shares reserved for retail investors. They provided finance to three key operators to make applications in the retail category of IPO's of IDFC Limited, Sasken Communications Technologies Limited and Suzlon Energy Limited. After the allotment of shares, the key operators transferred their shares in favour of Jayesh, who later disposed them. Through this transaction, Jayesh, and his associates earned a profit of 4.04 crore through their fictitious assets.

SEBI, while investigating the 'YES Bank Scam', found that certain persons illegally obtained IPO's shares, which were reserved for retail investors through opening of numerous demat accounts in fictitious names. The investigation revealed that the person who opened the Benami demat accounts, transferred the shares to financers to make windfall gains from the difference in the price of the IPO and the listing price. It involved manipulation of the primary market, by financers and market players by opening fictitious or benami demat accounts.

The SEBI froze these fictitious demat accounts and the Income Tax Department scrutinised over 6.5 lakh demat accounts, which were frozen by SEBI after investigating 2006 IPO scams. The government had found that an amount of 1,200 crore was lying in the frozen accounts. The

Income Tax Department also found that the two major accused, Panchal and Sugandh Investments, had made 60.62 crore in one and a half years, while Jayesh P. Khandwala earned 4.04 crore. The capital market regulator, the SEBI after investigating the above IPO scams had made it mandatory for depository participants and later investors to quote Permanent Account Number (PAN) for operating demat accounts. The SEBI also directed Jayesh to disgorge the unlawful gain of 4.04 crore and directed him to pay a sum of 1.21 crore as interest.

## The Satyam Case (2009)

Probably the biggest corporate scam in India came from one of the largest IT companies in India and, ironically, the company involved was Satyam Computer Services, which means 'truth' (in Sanskrit). The Satyam founder, B. Ramalinga Raju, who was the Chairman of the company, confessed in his four-page letter to cooking up the books of accounts of the company and admitted that the accounting entries had been hugely inflated, resulting in a fraud involving about 8,000 crore.

The company did not have that much of money as it was showing for so many years. This was done to maintain the reputation of the company in the business circles, to keep getting its clients because of its strong liquidity position and to make the investors keep investing their money in the company. Raju had been manipulating the company's accounting numbers for years. He claimed that he overstated assets on Satyam's Balance Sheet by $ 1.47 billion. Satyam overstated the income nearly every quarter over the course of several years in order to meet analyst expectations. B. Ramalinga Raju and the company's global head of internal audit used a number of different techniques to perpetrate the fraud.

The fraud took place to divert the company's funds into the real-estate investments, keep high earnings per share, raise executive compensation and make huge profits by selling the stake at inflated price. The aborted Maytas acquisition deal was the last attempt to fill the fictitious assets with the real ones. Fortunately, the deal with Maytas was 'salvageable'. It could have been saved only if "the deal had been allowed to go through, as Satyam would have been able to use Maytas assets to shore up its own books." When the Maytas acquisition deal failed Raju confessed the fraud. The fabricated "Balance Sheet and Income Statement", shown in the Table given below, which shows the differences between the 'actual' and the 'reported' finances.

Fabricated Balance Sheet and Income Statement of Satyam as of September 30, 2008 ( in Crores)

| | Actual | Reported | Difference |
|---|---|---|---|
| Cash and Bank Balance | 321 | 5,361 | 5,040 |
| Accrued Interest on Bank FDs | Nil | 376.5 | 376 |
| Understated Liability | 1,230 | None | 1,230 |
| Overstated Liability | 2,161 | 2,651 | 490 |
| Total | Nil | Nil | 7,136 |
| Revenue (Q2 FY 2009) | 2,112 | 2,700 | 588 |
| Operating Profits | 61 | 649 | 588 |

(Source: European Journal of Business & Social Sciences March 2013, Page. 36)

This fraud was not committed overnight; it was building up continuously over the years. Besides the Chairman of the company, its auditors were also involved in this scam, as they ignored some of the obvious indications of embezzlement, and thus failed to catch on the massive scam, which could have been caught much before it acquired a massive status. The auditors [Price Waterhouse Coopers (PWC)] relied upon forged bank confirmation letters supplied by the other accused during the statutory audit and failed to verify the company's current account balance on-line as well as with the Bank Statement.

PWC audited the company for nearly 9 years and did not uncover the fraud whereas Merrill Lynch discovered the fraud as per the part of due diligence in nearly 10 days. As per the observations of the Central Bureau of Investigation, the 'blatant deviations' adopted by the auditors showed their underlying conspiracy' with the other key accused in the accounting fraud, which affected the

genuineness of the financial statement of the company. Besides overstating the balance, Raju has drew 20 crores monthly from the company as salary against non-existing employees as the company actually employed 40,000 employees while in record the number of employees was 53,000. He withdrew from the company the salary for these unrecorded employees and siphoned off the company's money for his personal use.

The following factors contributed to the fraud were greed, ambitious corporate growth, deceptive reporting practices - lack of transparency, excessive interest in maintaining stock prices, executive incentives, stock market expectations, nature of accounting rules, ESOPS issued to those who prepared fake bills, high risk deals that were sour, audit failures, aggressiveness of investment and commercial banks, rating agencies and investors, weak independent directors and audit committee and whistle-blowing policy not being effective.

The Satyam Computer Services scandal brought to light the importance of business ethics and its relevance to corporate culture. Satyam fraud spurred the government of India to tighten Central Government norms to prevent recurrence of similar frauds in the near future. The Satyam scandal has been perhaps the biggest example of corporate mis-governance in India in recent years.

The economic offences court on 9th January, 2014 convicted and sentenced to imprisonment to Ramalinga Raju's wife Nandini, sons Teja and Rama and wives of Raju's younger brothers among 84 directors convicted for evading income tax of around  30 crore. All male directors sentenced to one-year jail term, women directors given six months. However, on the same day special judge M Laxman suspended the sentence for a month to enable the convicted persons to seek remedial legal measures. Those convicted were directed to furnish sureties to avail of this facility. The convicted persons were asked to pay a penalty of  10,000 also. All of them paid the penalty and furnished the sureties after the pronouncement of the order.

In 2005, the market regulator, SEBI ordered B Ramalinga Raju and his family, the former promoters of fraud-ridden erstwhile Satyam Computers, to return  1,803 crore of their ill-gotten money plus interest for over six and-a half years, which adds upto about  3,200 crore. Raju and some of his family members have also been banned from the market for seven years. SEBI ordered the Rajus to disgorge all their ill-gotten profits along with a simple interest at 12 per cent per annum since January 7, 2009 till the day of payment. The regulator also said since the IL and FS Engineering and Construction in its former avatar as Maytas Infra had made unlawful gains, which still remain with the company under the new management, those gains should be returned.

Six years, three months and two days after he confessed to having fudged his books what turned out to be one of India's biggest corporate scams, Satyam founder and former chairman, B. Ramalinga Raju was held guilty by a trial court and sentence and sentenced to seven years rigorous imprisonment and fined 5 crore Raju's brother, Rama was given a similar sentence and fine while the other eight accused got seven years, but levied lessor fines. All of them were convicted under Indian Penal Code Section 120B (criminal conspiracy) read with 420 (cheating). Raju was also convicted under 409 (criminal breach of trust by merchant or agents), 467 (forgery), 468 (forgery for the purpose of cheating), 471 (using as genuine a forged document), 477A (falsification of accounts) and 201 (destruction of evidence). The Enforcement Directorate has also booked a case against Satyam Computers Founder, B. Ramalinga Raju and then directors of the Company under various provisions of the Foreign Exchange Management Act (FEMA). Other convicted and sentenced were Vadlamani Srinivas, then chief financial officer at Satyam, and former Price Waterhouse auditors Subramani Gopalakrishnan and T. Srinivas. Subramani Gopalakrishnan and T. Srinivas was charged with colluding with Satyam founder. The US Securities and Exchange Commission penalized PwC- India, accused it of not following basic audit procedures. Firm asked to cough up $ 7.5 m in fine. The two were banned for life by Institute of Chartered Accountants of India. Their special leave petitions filed in apex court were dismissed.

After Satyam scam, the Government of India considered the scrutiny of role of auditors of the company to meet the needs of investors, management and society as a whole. The Central Government under the Companies Act, 2013 established the National Financial Reporting Authority (NFRA) to scrutinize the role of those Chartered Accountants who are associated with ensuring compliance with accounting standards and policies. The act also has provisions for rotation of auditors to avoid nexus between auditors and directors.

 Task

Discuss the Saradha Group-Chit Fund Case (2013).

## The Bank of Baroda Case (2015)

The Bank of Baroda (BOB) scam is a case of money-laundering as an amount of 6,172 crore was illegally remitted to Hong Kong and the UAE. The accused in this case were S K Garg, Assistant General Manager of the BOB; Jainesh Dubey, Foreign Exchange Officer of the BOB; Kamal Kalra, foreign exchange division of the HDFC Bank, Chandan Bhatia, Gurucharan Singh Dhawan and Sanjay Aggarwal, the promoters of Shell companies. These three persons, Chandan Bhatia, Gurucharan Singh Dhawan and Sanjay Aggarwal, incorporated 15 shell companies in India and abroad by appointing their low-paid employees as Directors. The accused, in connivance of the BOB officials, created a fraudulent trade circuit, where exporters claimed the duty drawback on inflated exports bills on non-existent imports. Through these 15 companies, they made payments for non-existent imports, like cashew, pulses, and rice. To make payments against the exports, the amount was deposited into 59 accounts of the Bank of Baroda, Ashok Vihar, of Delhi branch, in cash, as advance for imports. Amazingly, all the 59 accounts were opened from May, 2014, to June, 2015. The money was remitted to some of the companies in Hong Kong.

The camouflaged transactions were completed by these companies, and 59 accounts as Indian companies exported overvalued products by generating fake bills and the Hong Kong companies submitted forged import bills to claim the duty drawback. The Ashok Vihar branch of the BOB was a new branch which had obtained permission to accept forex transactions only in 2013. It transpired that, within a year, the forex business of the branch shot upto 21,529 crore. The BOB noticed some unusual transactions at its Ashok Vihar Branch. The bank officials alerted the government agencies who sprang into action and the CBI and the ED raided some branches of the BOB and residence of some of employees. The CBI found that an estimated 6,000 crore was transferred through nearly 8,000 transactions made from July, 2014 to July, 2015. The Enforcement Directorate too probed the case and participated in the searches conducted by the CBI.

On October 12, 2015, six persons, including Garg and Dubey were arrested on charges of criminal conspiracy, cheating and provisions of the Prevention of Infamous Corporate Frauds in India and Abroad Corruption Act. The other four arrested, included Kamal Kalra, working with the foreign exchange division of the HDFC bank, Chandan Bhatia, Gurucharan Singh Dhawan and Sanjay Aggarwal. The agency had conducted searches on the bank premises and the residences of Garg and Dubey. The Assistant General Manager, SK Garg and Jainish Dubey, were produced before the Special Judge of the CBI, Justice PK Jain where the agency sought their custodial interrogation for five days. They were later arrested for the alleged offences under the provisions of the IPC and the Prevention of Corruption Act.

Kalra confessed during questioning that he had helped Bhatia and Aggarwal in remitting a part of the over 6,000 crore amount through Bank of Baroda on a commission of 30:50 paise per dollar sent abroad through banking channels. The Enforcement Directorate attached properties worth 12.50 crore belonging to the four accused and their family members in the 6,000 crore BOB hawala scam. The Union Finance Minister Arun Jaitley said the magnitude of the alleged black money transfer through the state-owned BOB will only be known after completion of the multi-disciplinary probe.

## The PACL Case (2015)

PACL, formerly known as Pearls Agrotech Corporation Limited, founded by Nirmal Singh Bhangoo, had raised 49,100 crore from nearly 5 crore investors. PACL was engaged in a ponzi scheme as it was accepting money by investors with a promise to give agricultural land with a high returns to them. It purchased large land by the funds mobilised through ponzi scheme in 1990.

PACL alongwith it's another group company, Pearls Golden Forest Limited (PGFL) illegally mobilised deposits from public without any permission from the Reserve Bank of India. The company managed to lure the investors who would then become its agents by promises like 'double your money in Six years'. The money was collected by the company as investment from various depositors and later used to buy the land across the country. Both the companies, PACL and PGFL, were running a 'pyramid scheme' under the grab of agricultural land to the depositors. When the SEBI came to know about the PACL scheme in 1999, directed to PACL, to comply with the SEBI's Regulations dealing with Collective Investment Schemes (CIS).

The SEBI also raised concern over the legality of PACL's operations, since it was running a CIS in the garb of a real estate company. The company argued it was selling land to customers and not investment schemes, and was not therefore, subject to SEBI regulations. The SEBI first issued a notice to the PACL, stating that the company was operating CIS, where the funds of the investors were pooled and utilised towards the cost of land, registration and developmental charges, and incidental expenses. The case later went to courts, while the Supreme Court passed an order in February 2013, directing the SEBI to determine whether the business of PACL fell within the purview of the CIS or not, and take further action in accordance with the law.

The SEBI, in its order on 22 August 2014, ruled that "the business/activities/ schemes/plans offered and operated by PACL were Collective Investment Schemes, satisfying all the ingredients specified under Section 11AA of the Securities and Exchange Board of India Act, 1992". It also directed the company to wind up all its CISs and to refund the funds raised from investors. The PACL did not comply with the SEBI order and challenged the order in the higher appellate authority, i.e. the Securities Appellate Tribunal (SAT). The tribunal, in August 2015, upheld the market regulator's order against the company and directed the PACL to comply "with directions contained in the impugned order of SEBI within three months."

The SEBI in its order also observed that the officers of the PACL committed the crime repeatedly and mobilised a huge amount of money from which it earned a profit of more than 2,423 crore in less than a year. The SEBI imposed the highest ever fine of 7,269 crore on PACL for duping the investors. The fine imposed was equal to three times the profit earned by the company out of this transaction. The CBI, after 17 months of the SEBI's order to PACL to refund money to the investors, arrested Nirmal Singh Bhangoo, the founder of PACL on account of allegations that the company cheated the investors to the tune of $6.8 billion.

Three other officials of the PACL were later arrested for criminal conspiracy and cheating.

## Summary

According to the RBI data, corporate loans account for nearly 70% of these bad loans, while retail loans, which include car loans, home loans and personal loans, account for only 4%. The following are the primary reasons for increasing bank scams:

- Poor bank corporate governance- A study by the Indian Institute of Management Bangalore has shown that poor bank corporate governance is the cause behind rising bank scams and Non-Performing assets (NPAs).
- Limited monitoring- Research has shown that limited asset monitoring after disbursement and insufficient due diligence before disbursement were among the major factors for these NPAs.
- Involvement of management- Data by the RBI shows that around 34% of scams in the banking industry are on account of inside work and due to poor lending practices by and the involvement of junior and mid-level management.
- A high NPA reduces the net interest margin of banks besides increasing their operating cost and the banks meet this cost by increasing the convenience fee from their small customers on a day-to-day basis.
- Evaluation of borrower- Since bad loans lead to higher NPAs over time, banks have to exercise due diligence and caution while offering funds.
- Banks should be cautious while lending to Indian companies that have taken huge loans abroad.

The steps that need consideration to curb banking scam are:

- The CIBIL score of the borrower should be evaluated by the bank concerned and RBI officials.

- Auditing- The regulation and the control of chartered accountants is a very important step to reduce non-performing assets of banks.There is an urgent need to tighten the internal and external audit systems of banks.
- Rotation of employees- The fast rotation of employees of a bank's loan department is very important.
- Internal rating agency- Public sector banks should set up an internal rating agency for rigorous evaluation of large projects before sanctioning loans.
- Monitoring business projects- There is a need to implement an effective Management Information System (MIS) to monitor early warning signals about business projects.
- Use of ICT- Financial fraud can be reduced to a great extent by the use of artificial intelligence (AI) to monitor financial transactions.
- Fraud risk assessments- Banks need to carry out fraud risk assessments every quarter.
- Improved loan recovery- India has to improve its loan recovery processes and move beyond the National Asset Reconstruction Company Ltd. (NARCL) or the bad bank.

## Keywords

Capital Market: A capital market is a place where buyers and sellers indulge in trade (buying/selling) of financial securities like bonds, stocks, etc.

CBI: CBI stands for Central Bureau of Investigation, the main investigating agency of the Government of India.

CIBIL score: CIBIL Score is a three-digit number ranging from 300 to 900 which is used to assess your creditworthiness.

Demat Account: A demat account helps investors hold shares and securities in an electronic format. This kind of account is also called a dematerialised account.

IPO: An initial public offering (IPO) refers to the process of offering shares of a private corporation to the public in a new stock issuance for the first time.

Margin Trading: Margin trading refers to borrowing money from the broker to purchase stock. The investor is allowed to buy more securities than what he can afford with the available funds at the moment.

Mutual Fund: A mutual fund is a pool of money managed by a professional Fund Manager. It is a trust that collects money from several investors who share a common investment objective and invests the same in equities, bonds, money market instruments and/or other securities.

NPA: A non performing asset (NPA) is a loan or advance for which the principal or interest payment remained overdue for a period of 90 days.

RBI: The Reserve Bank of India, chiefly known as RBI, is India's central bank and regulatory body responsible for the regulation of the Indian banking system.

SEBI: SEBI stands for Securities and Exchange Board of India. It is a statutory regulatory body that was established by the Government of India in 1992 for protecting the interests of investors investing in securities along with regulating the securities market.

Short selling: Short selling occurs when an investor borrows security, sells it on the open market, and expects to buy it back later for less money.

## SelfAssessment

1. How does management generally commit corporate fraud?

A. in connivance with the unscrupulous professionals

B. in connivance with the ethical professionals

C. in connivance with the ethical auditors

D. in connivance with the ethical consultants

2. Which is the most common type of fraud in India?

A. Procedural lapses

B. Accounting fraud

C. Asset Misappropriation

D. Cash embezzlement

3. Why are most companies reluctant to take legal recourse against employees responsible for committing fraud?

A. To evade payments to the general public

B. To evade taxes

C. To evade payments to lawyers

D. Fear of loss of reputation

4. Companies are generally interested in recovering the defrauded money rather than getting the culprit punished.

A. True

B. False

5. Which of the following feature of corporate fraud suggests "Reliance on Internal and External Audits and code of conduct is the main measure to detect and prevent fraud which is insufficient for detecting and preventing frauds in today's hi-tech world"?

A. Insufficient Authorities

B. Insufficient Powers with Fraud Regulating Agencies

C. Lack of Action against Perpetrators

D. Weak Anti-fraud Measures

6. Identify the reason behind increasing banking scams from the following:

A. Involvement of management

B. Proper evaluation of borrower creditworthiness

C. Robust internal and external banking audit system

D. Rotation of employees

7. Identify the preventive measure to curb banking scams from the following:

A. Limiting asset monitoring after disbursement of loan

B. Effectively use of ICT

C. Improper evaluation of borrower credit rating

D. Weak bank corporate governance

8. Which is the biggest Indian Banking Fraud from the following?

A. ABG Shipyard Scam

B. Nirav Modi Scam
C. Vijay Mallya Scam
D. DHFL Scam

9. Nirav Modi is the prime fraudster in:

A. Andhra Bank Scam
B. IDBI Bank Scam
C. PNB Scam
D. Bank of India Scam

10. Vikram Kothari is the prime fraudster in:

A. ABG Shipyard Scam
B. Rotomac Pen Scam
C. Winsome Diamond Scam
D. Videocon Scam

11. Who earned the nickname of Big Bull of the trading floor?

A. Ketan Parekh
B. Harshad Mehta
C. CR Bhansali
D. Roopalben Panchal

12. Which of the following scam involved manipulation of the primary market by financers and market players by opening fictitious or benami demat accounts?

A. The Harshad Mehta Scam
B. The Satyam Scam
C. The IPO Demat Scam
D. The PACL Scam

13. Which of the following scam involved cooking up the books of accounts of the company resulting in fraud involving about 8,000 crore?

A. The Harshad Mehta Scam
B. The Satyam Scam
C. The IPO Demat Scam
D. The PACL Scam

14. Which of the following scam involved the use of Ponzi schemes?

A. The Saradha Group-Chit Fund Scam
B. The Ketan Parekh Scam
C. The CR Bhansali
D. The PACL Case

15. The following fraudster selected those companies for investment which were high growth companies with low capital base. He took advantage of the low liquidity in these stocks and these companies were known as 'K-10' stocks.

A. Ketan Parekh
B. Harshad Mehta
C. CR Bhansali
D. Roopalben Panchal

## Answers for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | A | 2 | B | 3 | D | 4 | A | 5 | D |
| 6 | A | 7 | B | 8 | D | 9 | C | 10 | B |
| 11 | B | 12 | C | 13 | B | 14 | A | 15 | A |

## Review Questions

1. Explain Vijay Mallya Fraud case.
2. Explain the two biggest Indian banking scams.
3. List 10 Indian Banking scams.
4. Explain the Rotomac Pen scam.
5. Discuss the Andhra Bank scam.
6. Explain the two biggest Indian capital market scam.
7. Discuss the CR Bhansali scam.
8. Examine the Ketan Parekh scam.
9. List any five Indian capital market scams.
10. Explan ABG Shipyard Fraud case.

## Further Readings

Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.

### Web links

https://www.indigolearn.com/blogs/Top-5-Financial-Scams-in-India/b218399bd14e4473907fdaa165b20f94

https://blog.ipleaders.in/top-10-biggest-scams-in-india/

https://www.iasparliament.com/current-affairs/banking-scams-in-india

https://insideiim.com/abg-shipyard-fraud-current-affairs

https://www.inventiva.co.in/trends/top-10-biggest-bank-frauds-in-india/

# Unit 06: Corporate Frauds Abroad

CONTENTS



## Objectives

After studying this unit, you will be able to:

- examine the mechanism of infamous corporate frauds happened in foreign countries.
- Evaluate the consequences of the infamous foreign corporate frauds.

## Introduction

A corporate scandal can have a dramatic effect on a company's bottom line. A corporate scandal can occur any time there is evidence of unethical behaviour, negligence or third-party interference that impacts a company's reputation. As we will see, this can include evidence of 'creative' accounting, dodgy business practices, data breaches or anything that damages the environment. In this unit, we take a look at the biggest corporate scandals that happened in foreign countries to explain how they affected each company's share price.

## 6.1 Infamous Corporate Frauds Abroad

### The Enron Case (1985)

The Enron Company was formed in 1985 and was one of the world's leading electricity, natural gas, pulp and paper, and communication company. Its demise was rooted in the fact that Jeff Skilling, the then president of Enron's trading operations, convinced federal regulators to permit Enron to use an accounting method known as 'mark to market'. This was the technique that was previously only used by brokerage and trading companies. With mark-to-market accounting, the price or value of security was recorded daily to calculate profits and losses. The use of this technique made it difficult to see how Enron was really making money. By using this method, Enron counted projected earnings from long-term energy contracts as current income. This was the technique used to inflate revenue numbers by manipulating projections for future revenues which increased the Enron stock prices. Enron had bought new venture that looked promising as a new profit centre and its acquisitions were growing exponentially. Enron had formed special purposes entities (SPES) which were known as 'off balance sheet entities' to move debt off of the balance sheet and transfer risk for their other business ventures. These SPES were also established to keep Enron's credit rating high, which was very important in their field of business. Because the executives believed Enron's long-term stock values would remain high, they looked for way to use the company's stock to hedge its investments in these other entities. The Raptors were established to cover their losses of

the stock in their start-up business. Enron suffered when the telecom industry suffered its first downturn. Business analysts began trying to unravel the source of Enron's money. The Raptors collapsed and Enron's stock fell below a certain point because they were ultimately backed only by work, but Enron used one of their SPES When Enron's stocks declined, the Raptors began to decline as well and Enron's

CEO, Jeff Skilling, resigned due to "Family Issues", while as per Enron's Vice- President, he had resigned due to accounting improprieties and other legal actions. This shocked both the industry and Enron employees, thereafter, Enron's chairman Ken Lay stepped in as CEO, who questioned Enron's accounting method and specifically cited the Raptors transactions. She noted that the SPES had been controlled by Enron's CFO, Fastow, and that, he and other Enron employees had made their money and left Enron at risk for the support of the Raptors. (The Raptor deals were written such that Enron was required to support them with its own stock.) When Enron's stock fell below a certain point, the Raptors' losses began to appear on Enron's financial statements, and also a broker sent an e-mail to 73 investment clients, saying that Enron was in trouble and advised them to consider selling their shares.

The Stock Exchange Corporation (SEC) began an investigation into Enron's accounting procedures. Enron officials admitted to overstating company earnings by $57 million and Enron, or the 'crooked E', filed for bankruptcy in December 2001.

Enron's CFO was behind the complex network of partnerships, and many other questionable practices. He was charged with 78 counts of fraud, conspiracy, and money laundering. He accepted and pleaded guilty to two counts of conspiracies, he was given a 10-year prison sentence and ordered to pay $23.8 million in exchange for testifying against other Enron executives. Enron's CEO was convicted of 19 counts of conspiracies, fraud, insider trading and making false statements, while Enron's Chairman was convicted of six counts of conspiracies and fraud. In a separate trial, Lay was also found guilty of four counts of bank fraud. This case revealed that Enron's reported financial condition was sustained mostly by institutionalised, systematic, and creatively planned accounting fraud. Enron has since become a proper symbol of wilful corporate frauds and corruption.

## The World Com Case (2002)

In the WorldCom case, the CFO and the controller committed securities fraud and filed a false return to SEC. The CFO adopted a series of accounts adjustment and took a personal loan from the Corporation's fund. The SEC levied charges against the corporation's CEO and several executives, and during the yearlong investigation into WorldCom's accounts, nine billion dollars in discrepancies were found.

Coming hot on the heels of accounting scandals involving Enron and Tyco, both of which sent financial markets into tailspins, the fraud committed by WorldCom, one of the world's biggest telecommunications companies, ended up dwarfing even those infamous crimes in terms of sheer numbers.By June 2002, the United States' second-largest long-distance telecommunications company confirmed it had overstated its earnings, mainly by classifying as capital expenditures those payments it was making for using the communications networks of other companies.

WorldCom had "cooked the books" repeatedly—including its income statement, balance sheet, Form 10-K filing and annual report—in its attempts to inflate its profit-and-loss position by a whopping $3.8 billion, with senior management well aware of the skullduggery being committed. It became the biggest accounting scandal on record in the US and was one of the biggest ever bankruptcies filed.

And as a result of the company's actions, Chief Executive Officer Bernard Ebbers was sentenced to 25 years in prison, while the company's chief financial officer, Scott Sullivan, received five years behind bars. But things had been so markedly different just a few years before. WorldCom had experienced stellar growth throughout much of the 1990s, mainly by achieving several highly profitable strategic acquisitions of other telecommunications companies, including MCI Communications—a company with 2.5 times larger revenue than WorldCom—for $37 billion in 1998. It then moved aggressively into internet communications, and by 2001, it was handling half of all internet and e-mail traffic in the US.

For this acquisition strategy to be successful, much depended on the company's stock price staying on a consistently upward trajectory. Until early 1999, the strategy seemed to be working for the

company—especially for Ebbers, who was worth an estimated $1.4 billion and had been named the 174th richest American on the Forbes 400.But that year saw WorldCom's revenue growth begin to slow, which in turn dragged down its stock price. This could partly be attributed to the vast oversupply of US telecommunications networks at the time, which overshot demand in the face of excessively bullish expectations surrounding the growth of the internet. And to compound matters, its proposed merger with Sprint Corporation was shut down that year based on antitrust concerns.

As such, there was much concern from Ebbers and senior management that WorldCom's earnings would not meet the expectations set by Wall Street analysts. In response, WorldCom began tampering with its financial statements to conceal its lacklustre performance and give the impression that it had met those analysts' projections.It reduced the amount it held in reserve by $2.8 billion and reclassified those funds as revenues; it then did the same with operating expenses that represented the amount WorldCom paid to other telecommunications companies to access their networks, "hiding" those expenses as long-term capital investments.

The reclassifications gave WorldCom an additional $3.85 billion—the changes making it appear as though the company had generated $1.38 billion in profits, along with heavily inflated assets.Ebbers continued to manage Wall Street expectations of double-digit growth by reporting the manipulated numbers and presenting the false impression of a thriving company to the market as well as internally to both the WorldCom employees and the board of directors. But he was receiving information internally that was wholly inconsistent with such an impression, particularly from CFO Sullivan and WorldCom's controller, David Myers. Indeed, much of the fraudulent activity was conducted under the direction of Sullivan.

As the company continued failing to meet the financial targets announced by Ebbers, Sullivan continued making false accounting entries to give the appearance that those targets were being achieved. And he was ably assisted by Myers, who similarly directed the making of unsupported entries.

Evidence also made clear that Ebbers was aware of the manipulations being undertaken by Sullivan and Myers, and Sullivan later confirmed that Ebbers knew of the capitalization of line costs. And yet, the chief executive continued to make unrealistic projections to the market and failed to disclose any of the internal dishonesty taking place.

Some believe this was the case because Ebbers was more concerned about protecting his vast personal wealth and his huge salary, which made him one of the country's highest-paid executives. By February 2002, WorldCom's results for the fourth quarter of 2001 were well below Wall Street expectations, and the company reduced its guidance for 2002.

But Ebbers still provided a very upbeat outlook for the company, saying, "We have solid investment grade debt ratings, and we are free cash flow positive" and "Let me be clear, we stand by our accounting". Nevertheless, Ebbers resigned in April after being told he would be dismissed by the board.Rating agencies subsequently downgraded WorldCom, with Moody's downgrade in May putting WorldCom's debt at junk status. WorldCom's Internal Audit Committee also undertook a review of the company's capital expenditures, despite opposition from Sullivan and Myers.

More personnel began questioning Sullivan and Myers about the dubious accounting entries before Myers finally admitted to internal auditors that he could not support the capitalization of line costs. Once the Audit Committee was made aware of the irregularities, they duly terminated Sullivan and received Myers' resignation.

On June 25, 2002, WorldCom disclosed to the U.S. Securities and Exchange Commission (SEC) and the public that for 2001 and the first quarter of 2002, it had determined that certain transfers amounting to $3.852 billion from "line cost" expenses to asset accounts were not made following generally accepted accounting principles (GAAP).

The next day, the SEC filed a lawsuit against WorldCom shortly before the board of directors accepted a full, independent investigation of the accounting practices that occurred. Hearings were also held by the House Committee on Financial Services and the Senate Committee on Commerce, Science, and Transportation.

In total, WorldCom made more than $9 billion in erroneous accounting entries to achieve the impression it was making profits. It was orchestrated by a few key members of senior management based in the company headquarters in Mississippi and executed by employees in the financial and accounting departments across various locations.

The fraud was implemented by and under the direction of WorldCom's Chief Financial Officer, Scott Sullivan. As business operations fell further and further short of financial targets announced by Ebbers, Sullivan directed the making of accounting entries thathad no basis in generally accepted accounting principles to create the false appearance that WorldCom had achieved those targets," according to the SEC's report of the investigation.

"In doing so he was assisted by WorldCom's Controller, David Myers, who in turn directed the making of entries he knew were not supported."The SEC concluded that the scandal was very much the result of the way CEO Ebbers ran WorldCom. He was at the heart of the company's culture and exerted much of the pressure that led to the fraud lasting as long as it did. A lack of controls within the financial system at the time also played a major contributory role in the fraud.

As the SEC reported, the improper accounting entries were easily accomplished because "it was considered acceptable for the General Accounting group to make entries of hundreds of millions of dollars with little or no documentation beyond a verbal or an e-mail directive from senior personnel".

The SEC also highlighted the part played by Arthur Andersen's grossly inadequate auditing, and while there was insufficient evidence that WorldCom's auditing firm during the fraud period was aware of the capitalization of line costs or that WorldCom's revenues were being improperly reported, there were clear flaws in Andersen's audit approach, which limited the likelihood it would detect the accounting irregularities.

"Andersen appears to have missed several opportunities that might have led to the discovery of management's misuse of accruals, the capitalization of line costs, and the improper recognition of revenue items," the SEC report stated.

"For their part, certain WorldCom personnel maintained inappropriately tight control over information that Andersen needed, altered documents with the apparent purpose of concealing from Andersen, knowing in some instances that it was receiving less than full cooperation on critical aspects of its work, failed to bring this to the attention of WorldCom's Audit Committee."Andersen items that might have raised questions, and were not forthcoming in other respects.

The regulator also cited "a lack of courage" by others in WorldCom's financial and accounting departments to blow the whistle. "Employees in the financial and accounting groups believed that forcefully objecting to conduct that they knew was being directed by Sullivan would cost them their jobs; few of them were prepared to take that risk."

That said, the SEC did acknowledge that some did make complaints to their supervisors as well as refused to take certain actions they considered inappropriate. Nonetheless, no one took the necessary action to halt or expose the ongoing practices until the spring of 2002.

## The Tyco Case (2005)

Tyco CEO Dennis Kozlowski and CFO Michael Swartz faced criminal charges for taking private loans from Tyco for over 170 million dollars. The loans, many of which were interest-free or fully forgiven, were not revealed to shareholders. Mark Belnick, Tyco's former General Counsel, was also charged for receiving fourteen million dollars in loans for houses he purchased in New York and Utah. The corporation removed Kozlowski, Swartz, Belnick and other members from its board of directors, and replaced them with professionals from outside as Edward Breen, David Fitzpatrick, and William Lytton, who re-established Tyco's management board and the company moved towards recovery.

## The Ponzi Scheme (Fort Lauderdale) Case (2009)

Scott Rothstein, an attorney, in Fort Lauderdale, Fla. engaged in a pattern of racketeering activity, through the defunct Ft. Lauderdale law firm of Rothstein Rosenfeldt and Adler, PA (RAA). RRA fraudulently obtained approximately $1.2 billion from investors through bogus investments and other schemes. Rothstein used RRA to fraudulently induce investors to (1) loan money to non-existent borrowers based upon promissory notes, and requested short-term bridge loans for business financing; and (2) invested funds based upon anticipated payouts from purported confidential civil settlement agreements. Rothstein falsely represented to the investors that the

purported clients were willing to pay high rates of return on these loans. Rothstein and other co-conspirators solicited clients to invest in purported civil case settlement funds. Investors were falsely told that these settlements ranged in amounts from hundreds of thousands to millions of dollars. He further convinced the investors, that these settlements could be purchased at a discount, and would be repaid over time to them at full face value. In addition, investors were told that these funds would be held in the trust's account of RRA. The purported investment vehicles never existed, but were part of an elaborate Ponzi scheme in which new investors' money was used to repay money owed to earlier investors. To conceal the fraud, Rothstein and his co-conspirators created false bank documents, false online bank account information, false settlement agreements, and promissory notes. Rothstein and others defrauded clients of RRA in a civil suit initiated by RRA on their behalf as plaintiffs. Without the clients' knowledge, RRA settled the lawsuit in favour of the defendant, thereby obligating the clients to pay $500,000 to the defendant in the civil lawsuit. To carry out the fraud, Rothstein and co-conspirators created a false federal court order, purportedly signed by a U.S. District Judge, stating that the clients had won the lawsuit and owed a judgment of approximately $23 million. The false court order also stated that the defendant in the civil suit had transferred the funds to the Cayman Islands, to avoid paying the judgment. Rothstein and others falsely advised the clients that to recover those funds, the clients were required to post bonds. In this way, Rothstein caused the clients to wire transfer approximately $57 million to a trust account he controlled, purportedly to satisfy the bonds. Rothstein and other co-conspirators used the funds obtained through the Ponzi scheme for their benefit. In 2010, Scott Rothstein, an attorney, was sentenced to 60 months in prison, to be followed by three years of supervised release. Rothstein had previously been issued an order to forfeit his interests in real property, vehicles, bank accounts, and investments.

## The Mark Todd Case (2002-2005)

Mark Todd Hauze was convicted by the court as guilty of mail and wire fraud, and false statements on the tax returns. He used sales agents, a website, and other means to fraudulently solicit more than $10 million from members of the public, supposedly for participation in foreign currency trades. He convinced people to invest their retirement accounts and other funds in Universal Money Traders (UMT) by falsely representing, among other things, that UMT's foreign currency trading had generated annual returns of 30 percent or more, that UMT used a guaranteed "stop-loss" system which limited a client's potential losses, and also that clients would be able to check their account balances and trading results on readily-accessible, accurate, online account statements. He intentionally concealed from UMT's clients that UMT did not actually use a guaranteed stop-loss and that UMT regularly reported bogus trading results and false account balances to the clients. The false trading reports led UMT clients to believe that their account balances were growing, whereas, in fact, Hauze had lost substantial amounts of the clients' funds through trading, commission charges, and other means. He used a substantial portion of the client's funds for his own personal gain, including luxury vehicles and sports gambling, and that he used new money received from UMT clients to fulfil withdrawal requests made by other clients. UMT failed to honour withdrawal requests made by their clients, which Hauze falsely claimed to be due to the client accounts being temporarily frozen for an audit. Hauze also attempted to hide nearly $900,000 of income from the Internal Revenue Service. A federal jury found Mark Todd Hauze guilty on January 26, 2010. He was sentenced to serve 108 months in federal prison and three years of supervised release.

## The President of California Agribusiness Case (1999-2002)

Curtis Leigh Parry, California, pleaded guilty on to three counts of tax evasion and three counts of filing false corporate income tax returns. He admitted that he was the sole shareholder and owner of Salinas Valley Engineering & Manufacturing, Inc., (SVEM), a corporation in the business of manufacturing selling and repairing agricultural equipment. He admitted that he knowingly diverted money from SVEM to himself through various fraudulent schemes. Parry told SVEM customers to pay him directly for work or materials provided by SVEM. He then deposited those cheques directly into his personal bank account. He also deposited third-party cheques payable to SVEM into his personal bank accounts. Parry also admitted in his plea agreement that he wrote numerous SVEM corporate cheques payable to himself and deposited those cheques into his personal bank accounts. He diverted SVEM funds to pay b personal expenses on various credit cards and used the SVEM corporate American Express card to make personal purchases for himself

and his family members. Parry failed to report any of the above-mentioned diverted funds as income on his personal income tax returns. The diversion of SVEM funds resulted in Parry filing false corporate income tax returns for SVEM. Parry agreed that the total tax loss of SVEM's corporate income tax returns was $93,435 and he wired more than $300,000 in diverted SVEM corporate funds overseas in an attempt to make his tax fraud difficult to detect. Parry conducted many of these transfers in structured transactions in amounts of less than $10,000 to avoid currency transaction report requirements. In 2010, Curtis Leigh Parry was sentenced to 18 months in prison, to be followed by three years of supervised release, and ordered to pay $221,641 in restitution.

### The Maximum Dynamics Case (2000-2005)

Eric Richfield Majors formed a company, Maximum Dynamics, formerly Basel in Colorado Springs became a publicly-traded company subject to SEC reporting in August 2002. Between August 2000 and April 2005, Majors and co-defendant Joshua Wolcott conspired to cause materially false information to be included in Maximum Dynamics' quarterly and annual statements and other reports and documents filed with the SEC. Majors and Wolcott used the names and identities of unwitting Mexican nationals and shell companies to issue stock compensation for consulting services purportedly done for the company. They maintained control of this stock, sold the stock and used the proceeds for their own enrichment and purposes. They sold Maximum Dynamics stock issued Mexican nominees on the open market, through brokerage accounts were opened in the names of the nominees, to individual investors or entities through private sales arranged, at the direction or on behalf of Majors and/or Wolcott. They would then use the proceeds of the stock sales for their own personal use and personal expenses, to make payments to relatives and pay for their personal expenses, to pay Maximum employees and bona fide Maximum consultants for their work for Maximum or for other expenses incurred in connection with developing the business of Maximum. As a result of the net proceeds realised by the defendants from the sale of Maximum and non-Maximum stock, that was sold in the names of the Mexican nominees, the government calculates the unpaid tax of $402,004, based on the realised gains of $1,262,258. In 2010, Eric Richfield Majors was sentenced to 60 months in prison for the conspiracy to defraud the Internal Revenue Service (IRS) and the U.S. Securities and Exchange Commission (SEC), and to three years of supervised release and was ordered to pay $127,239 in restitution to company shareholders and investors, and $39.301 in restitution to the IRS.

## 6.2 The Corporate Funding Financial of America Case (2001)

Richard Habib and Luis Madrid, President and Vice-President of Corporate Funding Financial of America, Inc. (CFFA), defrauded investors through their real estate finance and development company, CFFA. They conspired to commit mail and wire fraud and one count of filing a false tax return. They represented CFFA to the public and potential investors as a successful real estate investment company that had the capacity to develop profitable commercial and residential projects, including the "Finestra Lofts" development in the Little Italy section of downtown San Diego. They offered investors secured and unsecured promissory notes with yearly returns ranging from 14 to 96 percent. Habib admitted that: (a) he and Madrid misled investors about the success of CFFA as a real estate development company; (b) a large percentage of investors' funds were not invested in CFFA's real estate projects as represented to investors; (c) CFFA was paying the high rates of returns to investors with new money and not profits from the projects; (d) subordination agreements relating to Deeds of Trust that had been executed in favour of investors were forged, and (e) investor money was diverted for personal use. Habib admitted to defrauding investors of up to $20 million; Madrid admitted to defrauding investors of up to $50 million. Both admitted that they made false statements on their tax returns by not reporting all of the money they received from CFFA on their personal tax returns. Habib failed to report the income he received from CFFA on his 2003, 2004, and 2005 tax returns and admitted that the tax loss to the United States from his false statements was $293,108. Madrid failed to report the income he received from CFFA on his 2005 tax return, and admitted that the tax loss to the United States from his false statements was $89,963. In 2010, they were sentenced for their roles in connection with a scheme to defraud investors through their real estate finance and development company, Corporate Funding Financial of America, Inc. (CFFA). Habib was sentenced to 46 months in prison and three years of supervised release and Madrid was sentenced to 96 months in prison and three years of supervised release.

## The Edward Ehee Case (2001-2006)

Edward S. Ehee, defrauded investors through investment fund by tax evasion, making and subscribing a false partnership return of more than $4 million. Ehre represented to investors that he would invest their funds in the securities markets and employ complex trading strategies to earn high returns with less risk than is ordinarily associated with such returns. Instead of investing the funds as promised, he diverted most of the funds for improper purposes, including the payment of existing investor distribution obligations using new contributions from other investors, and payments for the benefit of himself and his family. Ehee also admitted that although he had approximately $240,500 in taxable income in 2005, he did not file a tax return or pay any income tax for 2005. Ehee also admitted that he made and subscribed under the penalties of perjury, a false partnership return for the tax year 2005 for one of his investment funds. He intentionally inflated the assets reported on the balance sheet of the return to match the amount of money that he was supposed to have invested on behalf of his clients, when he knew that he had not invested any of their money in that fund in 2005. In 2010, Edward S. Ehee was sentenced to 51 months in prison, to be followed by three years of supervised release, and ordered to pay restitution for committing wire fraud, tax evasion and making and subscribing to a false partnership return.

## The Fisher Sand & Gravel Co. Case (2009)

Michael Fisher, a former co-owner of Fisher Sand & Gravel Co. Inc. (FSG) pleaded guilty to conspiracy to defraud the United States by impeding the IRS, aiding in the filing of false federal tax returns for FSG, and filing false individual tax returns. According to court documents and testimony, Fisher caused FSG employees to pay for personal expenses such as construction expenses and furnishings for his personal residence and a recreation building, construction expenses for improvement to a gas station owned and controlled by Fisher, a well as household and utility bills, vacations, credit card bills and legal expenses for him and other Fisher family members. These payments for Fisher were never reported to the IRS, they were deducted on the FSG corporate income tax returns, and Fisher failed to report all of his income on his individual income tax returns. In 2009, Michael Fisher was sentenced to 37 months in prison, ordered to pay $90,000 fine and pay restitution of $308,069.

Two other FSG corporate officers were sentenced for their part in the conspiracy Amiel Schaff, FSG's former chief financial officer, and Clyde Frank, FSG's former comptroller, were both sentenced to 12 months probation with a condition of home confinement, fined $1,000, and ordered to complete 20 hours of community service by speaking to college students about the criminal offense to which they pleaded guilty and corporate frauds in general. In May 2009, the United States reached a deferred prosecution agreement with FSG in which FSG admitted responsibility for defrauding the United States. The agreement required FSG to pay a total of $1.16 million in restitution, penalties and fines, implement measures to prevent future fraud at the company and cooperate with the IRS in audits of its tax returns. Under that agreement, prosecution against FSG was deferred until December 2011.

## The Marian Gardens Tree Farm Case (2007)

Gary Ernest Williams, Chief Financial Officer, worked for Marian Gardens Tree Farm in Groveland (Florida), for about 20 years. In recent years, he had served as the company's Chief Financial Officer and used this position of trust to embezzle $10.5 million worth of funds from the company by falsifying cheques, taking out a business credit card in the company's name, and making large cash withdrawals that he told bank officials were to be used to pay "employee bonuses." Instead, Williams had deposited the stolen funds into his personal accounts and then used them to fund a lavish lifestyle. In addition to stealing this money from his employer, Williams further failed to pay federal income taxes for $3,675,000 on the illegally obtained funds. In 2009, Gary Ernest Williams was sentenced to 96 months in prison and ordered to pay more than $14 million in restitution to the United States and his former employer, Marian Gardens Tree Farm. In addition, Williams was ordered to forfeit homes in Pennsylvania and North Carolina; a 2007 Lexus automobile; and cash payments that had been used to purchase property in the Bahamas.

## The Quality Trucking Case (2000-2002)

Gladys Nell Bishop, President of Quality Trucking, Inc. set up an accounting system at the company and maintained checking accounts at two different banks but only reported cheques deposited into one of the checking accounts to the IRS. The total unreported income for all three years was more than $500,000. In 2009, Gladys Nell Bishop was sentenced to 36 months in prison, one year of supervised release and was ordered to pay $584,688 in restitution to the Internal Revenue Service (IRS) for making false statements on her corporate tax returns for the years 2000, 2001 and 2002.

## The Philadelphia Academy Charter School Case (2009)

Kevin O'Shea, the former CEO of Philadelphia Academy Charter School, pleaded guilty and admitted that he stole between $400,000 and $1 million from PACS by: (1) using approximately $710,000 in PACS' funds to purchase a building in the name of his purported non-profit business; (2) demanding kickbacks from PACS vendors; (3) submitting for reimbursement at least $40,000 in fraud invoices for personal expenses; (4) billing approximately $50,000 worth of home repairs to PACS; (5) collecting approximately $34,000 in rent from entities unit PACS facilities; and (6) hiring a computer firm in an attempt to destroy comp evidence to obstruct this investigation. O'Shea also admitted to filing a false return for 2006 (IRIS, 2012). In 2009, Kevin O'Shea was sentenced to 37 months in prison for filing a false tax return, mail fraud, and theft from a federally-funded programme. O'Shea was also ordered to pay $900,000 in restitution, a $1,000 fine, and to forfeit $500,000.

## Waste Management Scandal (1998)

Waste Management Inc. is a publicly-traded US waste management company. In 1998, the company's new CEO, A Maurice Meyers, and his management team discovered that the company had reported over $1.7 billion in fake earnings.

The Securities and Exchange Commission (SEC) found the company's owner and former CEO, Dean L Buntrock, guilty, along with several other top executives. In addition, the SEC fined Waste Management's auditors, Arthur Andersen, over $7 million. Waste Management eventually settled a shareholder class-action suit for $457 million.

## HealthSouth Scandal (2003)

HealthSouth Corporation is a top US publicly traded healthcare company based out of Birmingham, Alabama. In 2003, it was discovered that the company had inflated earnings by over $1.8 billion. The SEC had previously been investigating HealthSouth's CEO, Richard Scrushy, after he sold $75 million in stock a day before the company posted a huge loss. Although charged, Scrushy was acquitted of all 36 counts of accounting fraud. However, he was found guilty of bribing then Alabama Governor, Don Siegelman, and was sentenced to seven years in prison.

## Freddie Mac Scandal (2003)

The Federal Home Loan Mortgage Corporation, also known as Freddie Mac, is a US federally-backed mortgage financing giant based out of Fairfax County, Virginia. In 2003, it was discovered that Freddie Mac had misstated over $5 billion in earnings. COO David Glenn, CEO Leland Brendsel, former CFO Vaughn Clarke, and former Senior Vice Presidents Robert Dean and Nazir Dossani had intentionally overstated earnings in the company's books. The scandal came to light due to an SEC investigation into Freddie Mac's accounting practices. Glenn, Clarke, and Brendsel were all fired and the company was fined $125 million.

## American International Group (AIG) Scandal (2005)

American International Group (AIG) is a US multinational insurance firm with over 88 million customers across 130 countries. In 2005, CEO Hank Greenberg was found guilty of stock price

manipulation. The SEC's investigation into Greenberg revealed a massive accounting fraud of almost $4 billion.

It was found that the company had booked loans as revenue in its books and forced clients to use insurers with whom the company had pre-existing payoff agreements. The company had also asked stock traders to inflate the company's share price. AIG was forced to pay a $1.64 billion fine to the SEC. The company also paid $115 million to a pension fund in Louisiana and $725 million to three pension funds in Ohio.



### Lehman Brothers Scandal (2008)

Lehman Brothers was a global financial services firm based out of New York City, New York. It was one of the largest investment banks in the United States. During the 2008 financial crisis, it was discovered that the company had hidden over $50 billion in loans. These loans had been disguised as sales using accounting loopholes.

According to an SEC investigation, the company had sold toxic assets to banks in the Cayman Islands on a short-term basis. It was understood that Lehman Brothers would buy back these assets. This gave the impression that the company had $50 billion more in cash and $50 billion less in toxic assets. In the aftermath of the scandal, Lehman Brothers went bankrupt.

### Bernie Madoff Scandal (2008)

Bernie Madoff is a former American stockbroker who orchestrated the biggest Ponzi scheme in history, and also one of the largest accounting scandals. Madoff ran Bernard L. Madoff Investment Securities LLC. After the 2008 financial crisis, it was discovered that Madoff had tricked investors out of over $64.8 billion.

Madoff, his accountant, David Friehling, and second in command, Frank DiPascalli, were all convicted of the charges filed against them. The former stockbroker received a prison sentence of 150 years and was also ordered to pay $170 billion in restitution.

**Task**: Discuss the Volkswagen emissions scandal.

## Summary

Corporate governance is a multi-level and multi-layered process that is distilled from an organization's culture, policies, values and ethics. It is an internal control in which responsibility is shared between the directors, the management and the employees. It is the responsibility of the Board of Directors to ensure that the company has an appropriate internal fraud-reporting mechanism, including arrangements for management monitoring and reporting. A transparent, ethical, and responsible corporate governance framework essentially emanates from the intrinsic will and passion for good governance. The global financial crises during the recent past, along with some of the large corporate failures and frauds, have revealed that while the corporate governance superstructure in India as well as other countries is fairly durable, certain weaknesses might have their roots in the ethos of the individual business firm.

There are some legal and regulatory obligations on companies to report fraud to third parties. Significant and material frauds need to be disclosed to the statutory auditors, shareholders, and investors. Despite good corporate governance and the existence of numerous legislations and regulatory authorities, corporate frauds appear to have been rampant throughout the country. A need was felt to streamline the existing legal and regulatory obligation to report fraud for compliance, consistency, transparency, clarity and cost. These cases might uncover changes needed to minimize corporate fraud and may help to restore investor confidence in the corporate sector. Another possible outcome might help to identify potential weaknesses in the internal control framework that would help restore the investor's confidence. As frauds are more prevalent in today's business world, a clear-cut policy regarding the prevention and control of fraud is an essential condition for any organization.

## Keywords

Corporate fraud: It refers to illegal activities undertaken by an individual or company that are done in a dishonest or unethical manner.

Financial Statement Fraud: It is the intentional misstatement of financial statements by omitting critical facts or disclosures, misstating amounts, or misapplying GAAP.

Fraud: Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

Kiting fraud: It involves concealing cash shortages by – transferring funds from one bank to another and – recording the receipt of on or before the balance sheet date and the disbursement after the balance sheet date.

Ponzi scheme: A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors.

SEC: The Securities and Exchange Commission (SEC) is a U.S. government agency created by Congress to regulate the securities markets and protect investors.

SPE: A Special Purpose Entity (SPE) is a company specially created to fulfil a narrow, specific purpose.

## SelfAssessment

1. Environmental Protection Agency (EPA) is related to which of the following scandal?

A. Lehman Brothers
B. Enron
C. Bernie Madoff
D. Volkswagen Emission

2. SEC stands for:

A. Securities Exchange Committee
B. Securities Exchange Commission
C. Securities and Exchange Commission
D. Securities and Exchange Committee

3. Richard Scrushy was charged with which accounting fraud?

A. The Ponzi Scheme
B. The HealthSouth Scandal
C. The Enron Case
D. The Tyco Case

4. Arthur Andersen acted as _____ for Waste Management Inc in the context of the Waste Management Scandal.

A. Auditors
B. Chartered Accounts
C. Bankers
D. Investment House

5. In the Quality Trucking Case, who was the fraud perpetrator and what was the action taken against him/her?

A. CEO and 5 years imprisonment
B. Investment Fund Manager and 4 years imprisonment
C. President and 3 years imprisonment
D. Promoters and 9 years imprisonment

6. The modus operandi of the Enron Scam was:

A. Diverting money from SVEM to personal accounts
B. Manipulating financial records
C. Filing false corporate tax returns
D. Convincing people falsely to invest in their Retirement Accounts and giving false tax return

7. Fraudulently inducing investors to obtain money through bogus investments and other schemes was the modus operandi of the _____.

A. The Fisher Sand & Gravel Co. Scam
B. WorldCom Scam
C. Fort Lauderdale Law Firm Scam
D. Marian Gardens Tea Farms

8. CEO Bernard Ebbers, the fraud perpetrator was sentenced to _____ in prison as a consequence of the WorldCom Scandal.

A. 5 years
B. 10 years
C. 15 years
D. 25 years

9. What was the mechanism of the Tyco Scam?

A. Involving in the Tax Fraud
B. Manipulating Financial Statements
C. Insider Trading
D. Taking Private Loans by CFO and CEO from the company without receiving appropriate approval from the company's compensation committee and notifying shareholders

10. Who was/were the fraud perpetrator in the Fort Lauderdale Law Firm Scandal?

A. CEO
B. Promoters
C. Board Members
D. President

11. What was the mechanism of the WorldCom Scam?

A. Involving in the Tax Fraud
B. Manipulating Financial Statements
C. Insider Trading

D. Taking Private Loans by CFO and CEO from the company without receiving appropriate approval from the company's compensation committee and notifying shareholders

12. The modus operandi of the Mark Todd (Mail and Wire) Scam was:

A. Diverting money from SVEM to personal accounts
B. Manipulating financial records
C. Filing false corporate tax returns
D. Convincing people falsely to invest in their Retirement Accounts through sales agents

13. The jury found Mark Todd Hauze guilty on January 26, 2010, and sentenced him to serve _____ in federal prison.

A. 36 months
B. 60 months
C. 108 months
D. 120 months

14. The Enron Scam happened in _____.

A. 1980
B. 1985
C. 2002
D. 2005

15. Kevin O'Shea, the fraudster of the Philadelphia Academy Charter School Case was sentenced to _____ in prison.

A. 24 months
B. 36 months
C. 37 months
D. 48 months

## Answers Self Assessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | D | 2 | C | 3 | B | 4 | A | 5 | C |
| 6 | B | 7 | C | 8 | D | 9 | D | 10 | B |
| 11 | A | 12 | D | 13 | C | 14 | B | 11 | C |

## Review Questions

1. Discuss any five foreign corporate frauds.
2. List any ten foreign corporate frauds.
3. Explain the mechanism of the Enron scam.
4. Examine the mechanism of the WorldCom scam.
5. Discuss the Ponzi Scheme (Fort Lauderdale) Case.
6. Discuss the following foreign scams:

a) Volkswagen Emission Scandal

b) Lehman Brothers Scandal

c) The Quality Trucking Case

d) The Edward Ehee Case

e) The Mark Todd Case

## Further Readings

Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.

Web Links

https://corporatefinanceinstitute.com/resources/accounting/top-accounting-scandals/

https://www.ig.com/en/news-and-trade-ideas/top-10-biggest-corporate-scandals-and-how-they-affected-share-pr-181101

# Unit 07: Financial Statement Fraud

CONTENTS



## Objectives

After studying this unit, you will be able to:

- examine the nature and problems of Financial Statement Fraud.
- examine the motivations for Financial Statement Fraud.
- evaluate the framework for detecting Financial Statement Fraud.
- summarize the ways of committing and detecting Financial Statement Fraud.

## Introduction

The stock and bond markets are critical components of a capitalist economy. The efficiency, liquidity, and resiliency of these markets depend on the ability of investors, lenders, and regulators to assess the performance of business organizations. Financial statements prepared by such organizations play a very important role in keeping capital markets efficient. They provide meaningful disclosures of where a company has been, where it is currently, and where it is going. Most financial statements are prepared with integrity and present a fair representation of the financial position of the organization issuing them. These financial statements are based on generally accepted accounting principles (GAAP) that guide the accounting for transactions. While accounting principles do allow flexibility, standards of objectivity, integrity, and judgment must always prevail.

Unfortunately, financial statements are sometimes prepared in ways that misrepresent the financial position and financial results of an organization. The misstatement of financial statements can result from manipulating, falsifying, or altering accounting records. Misleading financial statements cause serious problems in the market and the economy. They often result in large losses by investors, lack of trust in the market and accounting systems, and litigation and embarrassment for individuals and organizations associated with financial statement fraud. In the present unit, the nature, problems and motivations of Financial Statement Fraud along with the framework to detect the same are discussed.

## 7.1 The Problem of Financial Statement Fraud

### Financial Statement Fraud in Recent Years

Let's discuss an overview of several abuses that occurred in recent years to understand why the reasons behind such confidence crises in the corporate world worldwide.

- **Misstated financial statements and "cooking the books":** Examples included Qwest, Enron, Global Crossing, WorldCom, and Xerox, among others. Some of these frauds involved 20 or more people helping to create fictitious financial results and mislead the public.
- **Inappropriate executive loans and corporate looting:** Examples included John Rigas (Adelphia), Dennis Kozlowski (Tyco), and Bernie Ebbers (WorldCom).
- **Insider trading scandals:** The most notable example was Martha Stewart and Sam Waksal, both of whom were convicted of using insider information to profit from trading ImClone stock.
- **Initial public offering (IPO) favoritism, including spinning and laddering (spinning involves giving IPO opportunities to those who arrange quid pro quo opportunities, and laddering involves giving IPO opportunities to those who promise to buy additional shares as prices increase):** Examples included Bernie Ebbers of WorldCom and Jeff Skilling of Enron.
- **Excessive CEO retirement perks:** Companies including Delta, PepsiCo, AOL Time Warner, Ford, GE, and IBM were highly criticized for endowing huge, costly perks and benefits, such as expensive consulting contracts, use of corporate planes, executive apartments, and maids to retiring executives.

**Exorbitant compensation (both cash and stock) for executives:** Many executives, including Bernie Ebbers of WorldCom and Richard Grasso of the NYSE, received huge cash and equity-based compensation that has since been determined to have been excessive.

**Loans for trading fees and other quid pro quo transactions**: Financial institutions such as Citibank and JPMorgan Chase provided favorable loans to companies such as Enron in return for the opportunity to make hundreds of millions of dollars in derivative transactions and other fees.

**Bankruptcies and excessive debt**: Because of the abuses described above and other similar problems, seven of the ten largest corporate bankruptcies in U.S. history occurred in 2001 and 2002. These seven bankruptcies were WorldCom (largest at $101.9 billion), Enron (second at $63.4 billion), Global Crossing (fifth at $25.5 billion), Adelphia (six at $24.4 billion), United Airlines (seventh at $22.7 billion), PG&E (eight at $21.5 billion), and Kmart (tenth at $17 billion). Four of these seven involved financial statement fraud.

**Massive fraud by employees:** While not in the news nearly as much as financial statement frauds, there has been a large increase in fraud against organizations with some of these frauds being as high as $2 to $3 billion.

### Why these Problems Occurred

Each of the problems discussed above represents an ethical compromise. The explanations covered previously of why people commit other frauds apply to financial statement fraud as well. Recall that three elements come together to motivate all frauds: (1) a perceived pressure, (2) a perceived opportunity, and (3) the ability to rationalize the fraud as acceptable and consistent with one's personal code of ethics. Whether the dishonest act involves fraud against a company, such as an employee embezzlement, or fraud on behalf of a company, such as financial statement fraud these three elements are always present.

Every fraud perpetrator faces some kind of perceived pressure. Examples of perceived pressures that can motivate financial statement fraud are financial losses, failure to meet Wall Street's earnings expectations, or the inability to compete with other companies. Also, executive compensation in the form of stock options is often much higher than any other form of

compensation and can be in the tens of millions of dollars. As such, executives had enormous pressure to boost their stock value since a small increase in the stock price could mean millions of dollars of compensation for management.

Fraud perpetrators must also have a perceived opportunity or they will not commit fraud. Even with intense perceived pressures, executives who believe they will be caught and punished rarely commit fraud. On the other hand, executives who believe they have an opportunity (to commit and/or conceal fraud) often give in to perceived pressures. Perceived opportunities to commit management fraud include such factors as a weak board of directors or inadequate internal controls and the ability to obfuscate the fraud behind complex transactions or related-party structures. Some of the main controls that could eliminate the perceived opportunity for financial statement fraud include the independent audit and the board of directors. Because management can override most internal controls, the audit committee of the board of directors and the independent auditor often provide final checks on financial statement fraud.

Finally, fraud perpetrators must have some way to rationalize their actions as acceptable. For corporate executives, rationalizations to commit fraud might include thoughts such as "we need to protect our shareholders and keep the stock price high," "all companies use aggressive accounting practices," "it is for the good of the company," or "the problem is temporary and will be offset by future positive results."

The fraud triangle provides insights into why recent ethical compromises occurred. Nine factors came together to create what we call the perfect fraud storm. In explaining this perfect storm, we will use examples from recent frauds.

### *Element 1: A Booming Economy*

The first element of the perfect storm was the masking of many existing problems and unethical actions by the booming economy of the 1990s and early 2000s. During this time, most businesses appeared to be highly profitable, including many new "dot-com" companies that were testing new (and many times unprofitable) business models. These booming economic conditions allowed fraud perpetrators to conceal their actions for longer periods.

The booming economy also caused executives to believe their companies were more successful than they actually were and that their companies' success was primarily a result of good management. Academic researchers have found that extended periods of prosperity can reduce a firm's motivation to comprehend the causes of success, raising the likelihood of faulty attributions. In other words, during boom periods, many firms do not correctly ascribe the reasons behind their successes. Management usually takes credit for good company performance.

When company performance degrades, boards often expect results similar to those in the past without new management styles or actions. Since management did not correctly understand past reasons for success, it incorrectly thinks past methods will continue to be successful. Once methods that may have worked in the past because of external factors fail, some CEOs may feel increased pressure. In some cases, this pressure contributed to fraudulent financial reporting and other dishonest acts.

### *Element 2: Decay of Moral Values*

The second element of the perfect fraud storm was the moral decay that has been occurring in the United States and the world in recent years. Whatever measure of integrity one uses, dishonesty appears to be increasing.

Example

Numerous researchers have found that cheating in school, one measure of dishonesty, has increased substantially in recent years. While cheating in school is not necessarily directly tied to management fraud, it does reflect the general decay of moral values in society at large.

### *Element 3: Misplaced Incentives*

The third element of the perfect fraud storm was misplaced executive incentives. Executives of most fraudulent companies were endowed with hundreds of millions of dollars in stock options and/or restricted stock that put tremendous pressure on management to keep the stock price rising even at the expense of reporting accurate financial results. In many cases, this stock- based compensation far exceeded executives' salary-based compensation. For example, in 1997, Bernie Ebbers, the CEO of WorldCom, had a cash-based salary of $935,000. Yet during that same period, he was able to exercise hundreds of thousands of stock options, making millions in profits, and

receiving corporate loans totalling $409 million. These incentive packages caused the attention of many CEOs to shift from managing the firm to managing the stock price, which, all too often, resulted in fraudulent financial statements. As mentioned earlier, in addition to managing stock prices, executives also defrauded shareholders by backdating options to maximize their compensation.

### *Element 4: High Analysts' Expectations*

The fourth element of the perfect storm, and one closely related to the last, was the often unachievable expectations of Stock market analysts that targeted only short-term behavior.

### *Element 5: High Debt Levels*

The fifth element in the perfect storm was the large amounts of debt each of these fraudulent companies had. This debt placed tremendous pressure on executives to have high earnings to offset high-interest costs and to meet debt covenants and other lender requirements.

Example

During 2000, Enron's derivates-related liabilities increased from $1.8 billion to $10.5 billion.

### *Element 6: Focus on Accounting Rules Rather Than Principles*

Some believe that another element of the perfect storm was the nature of U.S. accounting rules. In contrast to accounting practices in many countries such as the United Kingdom and Australia, the U.S. generally accepted accounting principles (GAAP) are more rule-based than principles- based. One potential result of having rule-based standards is that if a client can find a loophole in the rules and account for a transaction in a way that is not specifically prohibited by GAAP, then auditors may find it hard to prohibit the client from using that method of accounting. Unfortunately, in some cases, the auditors helped their clients find loopholes or permitted them to account for transactions in ways that violated the principle of an accounting method but were within the rules. The result was that specific rules (or the lack of specific rules) were exploited for new, often complex financial arrangements, as justification to decide what was or was not an acceptable accounting practice.

 Example

Consider the case of Enron. Even if Arthur Andersen had argued that Enron's special purpose entities weren't appropriate, it would have been impossible for the accounting firm to make the case that they were against any specific rules. Some have suggested that one of the reasons it took so long to get plea bargains or indictments in the Enron case was because it was not immediately clear whether GAAP or any laws had actually been broken.

### *Element 7: Lack of Auditor Independence*

A seventh element of the perfect fraud storm was the opportunistic behavior of some CPA firms. In some cases, accounting firms used audits as loss leaders to establish relationships with companies so they could sell more lucrative consulting services.

### *Element 8: Greed*

The eighth element of the perfect storm was greed by executives, investment banks, commercial banks, and investors. Each of these groups benefited from the strong economy, the many lucrative transactions, and the apparently high profits of companies. None of them wanted to accept bad news. As a result, they sometimes ignored negative news and entered into bad transactions.

### *Element 9: Educator Failures*

Firstly, educators had not provided sufficient ethics training to students.

By not forcing students to face realistic ethical dilemmas in the classroom, graduates were ill-equipped to deal with the real ethical dilemmas they faced in the business world.

Secondly, educator failure was not teaching students about fraud.

Thirdly, educator failure is the way we have taught accountants and business students in the past. Effective accounting education must focus less on teaching content as an end unto itself and instead use the content as a context for helping students develop analytical skills.

## 7.2 Nature of Financial Statement Fraud

Financial statement fraud, like other frauds, involves intentional deceit and attempted concealment. Financial statement fraud may be concealed through falsified documentation, including forgery. Financial statement fraud may also be concealed through collusion among management, employees, or third parties. Unfortunately, like other fraud, financial statement fraud is rarely seen. Rather, fraud symptoms, indicators, or red flags are usually observed. Because what appear to be symptoms can be caused by other legitimate factors, the presence of fraud symptoms does not always indicate the existence of fraud. For example, a document may be missing, a general ledger may be out of balance, or an analytical relationship may not make sense. However, these conditions may be the result of circumstances other than fraud. Documents may have been legitimately lost, the general ledger may be out of balance because of an unintentional accounting error, and unexpected analytical relationships may be the result of unrecognized changes in underlying economic factors, Caution should be used even when reports of the alleged fraud are received because the person providing the tip or complaint may be mistaken or may be motivated to make false allegations.

Fraud symptoms cannot easily be ranked in order of importance or combined into effective predictive models. The significance of red flags varies widely. Some factors will be present when no fraud exists; alternatively, a smaller number of symptoms may exist when fraud is occurring. Many times, even when fraud is suspected, it can be difficult to prove. Without a confession, obviously forged documents, or a number of repeated, similar fraudulent acts (so fraud can be inferred from a pattern), convicting someone of financial statement fraud is very difficult. Because of the difficulty of detecting and proving fraud, investigators must exercise extreme care when performing fraud examinations, quantifying fraud, or performing other types of fraud-related engagements.

**Case Study**

Phar-Mor: An Example of Financial Statement Fraud

The Phar-Mor fraud is a good example of how financial statement fraud occurs Mickey Monus opened the first Phar-Mor store in 1982. Phar-Mor sold a variety of household products and prescription drugs at prices substantially lower than other discount stores. The key to the low prices was claimed to be "power buying," a phrase Monus used to describe his strategy of loading up on products when suppliers were offering rock-bottom prices. When he started Phar-Mor, Monus was president of Tamco, a family-held distributing company that had recently been acquired by the Pittsburgh-based Giant Eagle grocery store chain. In 1984, David Shapira, president of Giant Eagle, funded the expansion of Phar-Mor with $4 million from Giant Eagle. Shapira then became the CEO of Phar-Mor, and Monus was named president and COO. By the end of 1985, Phar-Mor had 15 stores. By 1992, a decade after the first store opened, 310 stores had been opened in 32 states, posting sales of more than $3 billion. Phar-Mor's prices were so low that competitors wondered how it could sell products so cheap and still make a profit, and it appeared that Phar-Mor was on its way to becoming the next Wal-Mart. In fact, Sam Walton once stated that the only company he feared in the expansion of Wal-Mart was Phar-Mor.

After five or six years, however, Phar-Mor began losing money. Unwilling to allow these shortfalls to damage PharMor's appearance of success, Monus and his team began to engage in creative accounting, which resulted in Phar-Mor meeting the high expectations of those watching the company. Federal fraud examiners discerned five years later that the reported pretax income for fiscal 1989 was overstated by $350,000 and that the year 1987 was the last year that Phar-Mor actually made a profit.

Relying on these erroneous financial statements, investors saw Phar-Mor as an opportunity to cash in on the retailing craze. Among the big investors were Westinghouse Credit Corp., Sears Roebuck & Co., mall developer Edward J. de Bartolo, and the prestigious Lazard Freres &Co. Prosecutors stated that banks and investors put $1.14 billion into the company, based on its fictitious financial statements.

To hide Phar-Mor's cash flow problems, attract investors, and make the company look profitable, Michael Monus and his subordinate, Patrick Finn, altered the inventory accounts to understate the cost of goods sold and overstate income. Monus and Finn used three different methods including account manipulation, overstatement of inventory, and accounting rules manipulation. In addition to the financial statement fraud, internal investigations by the

company estimated that management embezzled more than $10 million. Most of the stolen funds were used to support Monus' now-defunct World Basketball League.

In 1985 and 1986, well before the large fraud began, Monus was directing Finn to understate certain expenses that came in over budget and to overstate those expenses that came in under budget, making operations look efficient. Although the net effect of these first manipulations evened out, the accounting information was not accurate. Finn later suggested that this seemingly harmless request by Monus was an important precursor to the later extensive fraud.

Finn also increased Phar-Mor's actual gross profit margin from 14.2 percent to around 16.5 percent by inflating inventory accounts. The company hired an independent firm to count inventory in its stores. After the third-party inventory counters submitted a report detailing the amount and retail value of a store's inventory, Phar-Mor's accountants would prepare what they called a "compilation packet." The packet calculated the amount of inventory at cost. and journal entries were then prepared. Based on the compilation, the accountants would credit inventory to properly report the sales activity, but rather than record a debit to the Cost of Goods Sold, they debited so-called "bucket" accounts. To avoid auditor scrutiny, the bucket accounts were emptied at the end of each fiscal year by allocating the balance to individual stores as inventory. Because the related cost of goods sold was understated, Phar-Mor made it appear as if it were selling merchandise at higher margins. As the cost of sales was understated, net income was overstated.

Phar-Mor would regularly pressure vendors for large, up-front payments in exchange for not selling competitors' products. These payments were called "exclusivity payments," and some vendors paid up to $25 million for these rights. Monus would use this money to cover the hidden losses and pay suppliers. Instead of deferring revenue from these exclusivity payments over the life of the vendors' contracts-consistent with generally accepted accounting principles-Monus and Finn would recognize all the revenue upfront. As a result of this practice, Phar- Mor was able to report impressive results in the short run.

### Motivations for Financial Statement Fraud

Motivations to issue fraudulent financial statements vary. As indicated previously in the "perfect storm analysis," sometimes the motivation is to support a high stock price or a bond or stock offering. At other times, the motivation is to increase the company's stock price or for management to maximize a bonus. In some companies that issued fraudulent financial statements, top executives owned large amounts of company stock or stock options, and a change in the stock price would have enormous effects on their personal net worth. Sometimes, division managers overstate financial results to meet company expectations.

Many times, pressure on management is high, and when faced with failure or cheating, some managers will turn to cheat. In the Phar-Mor case, Mickey Monus wanted his company to grow quickly, so he lowered prices on 300 "price-sensitive" items. Prices were cut so much that items were sold below cost, making each sale result in a loss. The strategy helped Phar-Mor win new customers and open dozens of new stores each year. However, the strategy resulted in huge losses for the company, and rather than admitting that the company was facing losses

Mickey Monus hid the losses and made Phar-Mor appear profitable. While the motivations for financial statement fraud differ, the results are always the same-adverse consequences for the company, its principals, and its investors.

## 7.3 Framework for Detecting Financial Statement Fraud

Identifying fraud exposures is one of the most difficult steps in detecting financial statement, fraud. Correctly identifying exposures means that you must clearly understand the operations and nature of the organization you are studying as well as the nature of the industry and its competitors. Investigators must have a good understanding of the organization's management and what motivates them. Investigators must understand how the company is organized and be aware of the relationships the company has with other parties and the influence that each of those parties has on management. In addition, investigators and auditors should use strategic reasoning when attempting to detect fraud.

**Did you Know?**

What is Strategic Reasoning?

Strategic reasoning refers to the ability to anticipate a fraud perpetrator's likely method of concealing a fraud. Because external auditors are charged with the responsibility for detecting material financial statement fraud, we take the perspective of how an external auditor should engage in strategic reasoning. However, this reasoning process can also occur when internal auditors, the audit committee, fraud investigators, or others are considering efforts to detect management fraud.

When engaged in strategic reasoning, an auditor will consider several questions, including the following:

1. What types of fraud schemes is management likely to use to commit financial statement fraud? For example, is management likely to improperly record sales before goods have been shipped to customers?

2. What typical tests are used to detect these schemes? For example, auditors often examine shipping documents to validate shipments to customers.

3. How could management conceal the scheme of interest from the typical test? For example, management may ship goods to an off-site warehouse to be able to provide evidence of shipment to an auditor.

4. How could the typical test be modified to detect the concealed scheme? For example, the auditor may gather information about the shipping location to ensure that it is owned or leased by the customer or interview shipping personnel to determine if sold goods are always shipped to the customer.

Fraudulent financial statements are rarely detected by analyzing the financial statements alone. Rather, financial statement fraud is usually detected when the information in the financial statements is compared with the real-world referents those numbers are supposed to represent, and the context in which management is operating and being motivated. Fraud is often detected by focusing on the changes in reported assets, liabilities, revenues, and expenses from period to period or by comparing company performance to industry norms.

**Example**

In the ZZZZ Best fraud case, for example, each period's financial statements looked correct. Only when the change in assets and revenues from period to period was examined and when assets and revenues reported in the financial statements were compared with actual building restoration projects was it determined that the financial statements were incorrect.

In addition to the typical analyses of financial statements (e.g., ratio, horizontal, and vertical analyses), research suggests that auditors, investors, regulators, or fraud examiners can benefit by using nonfinancial performance measures to assess the likelihood of fraud.

Even in HealthSouth Scandal, the risk of financial fraud was observed as high because the company's financial statement data were inconsistent with its nonfinancial measures as pointed by Prosecutor Colleen Conry during the trial.

The use of financial and non-financial data for detecting fraud is one of four key considerations in a framework for detecting fraud.

## Fraud Exposure Rectangle

| | |
|---|---|
| 1. Management and Directors | 2. Relationship with others |
| 3. Organization and Industry | 4. Financial Results and Operating characteristics |

The fraud exposure rectangle shown in the above Figure is a useful tool for identifying management fraud exposures. On the first corner of the rectangle are the management and directors of the company. On the second corner are relationships the company has with other entities. On the third corner are the nature of the organization being examined and the industry in

which the organization operates. On the fourth corner are the financial results and operating characteristics of the organization.

Although CPAs and others have traditionally focused almost entirely on financial statements to detect financial statement fraud, each of these four areas should be considered to effectively assess the likelihood of fraud. We now examine each of these four areas individually.

## Management and the Board of Directors

Top management is almost always involved when financial statement fraud occurs. Unlike embezzlement and misappropriation, financial statement fraud is usually committed by the highest individuals in an organization, and most often on behalf of the organization as opposed to against the organization. Because management is usually involved, management and the directors must be investigated to determine their exposure to and motivation for committing fraud. In detecting financial statement fraud, gaining an understanding of management and what motivates them is at least as important as understanding the financial statements. In particular, three aspects of management should be investigated as follows:

1. Managements' backgrounds

2. Managements' motivations

3. Managements' influence in making decisions for the organization

### *Managements' Backgrounds*

Concerning backgrounds, fraud investigators should understand what kinds of organizations and situations that management and directors have been associated with in the past.

An example of the importance of understanding management's background is the Lincoln Savings and Loan fraud. Before perpetrating the Lincoln Savings and Loan fraud, Charles Keating was sanctioned by the Securities and Exchange Commission for his involvement in a financial institution fraud problem in Cincinnati, Ohio, and, had signed a consent decree with the SEC that he would never again be involved in the management of another financial institution.

### *Managements' Motivations*

What motivates directors and management is also important to know. Is their personal worth tied up in the organization? Are they under pressure to deliver unrealistic results? Is their compensation primarily performance-based? Do they have a habit of guiding Wall Street to higher and higher expectations? Have they grown through acquisitions or through internal means? Are there debt covenants or other financial measures that must be met? Is management's job at risk?

These questions are examples of what must be asked and answered to properly understand management's motivations. Many financial statement frauds have been perpetrated because management needed to report positive or high income to support stock prices, show positive earnings for a public stock or debt offering, or report profits to meet regulatory or loan restrictions.

### *Managements' Influence in Making Decisions for the Organization*

Finally, management's ability to influence decisions for the organization is important to understand because perpetrating fraud is much easier when one or two individuals have primary decision-making power than when an organization has a more democratic leadership. Most people who commit management fraud are first-time offenders, and being dishonest the first time is difficult for them. For two individuals to simultaneously be dishonest is more difficult, and for three people to simultaneously be dishonest is even more difficult. When decision-making ability is spread among several individuals, or when the board of directors takes an active role in the organization, fraud is much more difficult to perpetrate. Most financial statement frauds do not occur in large, historically profitable organizations. Rather, they occur in smaller organizations where one or two individuals have almost total decision-making ability, in companies that experience unbelievably rapid growth, or where the board of directors and audit committee do not take an active role. An active board of directors and/or audit committee that gets involved in the major decisions of the organization can do much to deter management fraud. In fact, it is for this reason that NASDAQ and NYSE corporate governance standards require that the majority of board members be independent and that some of the key committees, such as audit and compensation, be comprised entirely of independent directors.

Once management decides that it will commit fraud, the particular schemes used are often determined by the nature of the business's operations. While we usually focus on the schemes and the financial results of those schemes, remember that the decision to commit fraud in the first place was made by management or other officers. Some of the key questions that must be asked about management and the directors are as follows:

**Understanding Management and Director Backgrounds**

1. Have any of the key executives or board members been associated with other organizations in the past? If so, what was the nature of those organizations and relationships?

2. Were key members of management promoted from within the organization or recruited from the outside?

3. Have any key members of management had past regulatory or legal problems, either personally or in organizations with which they have been associated?

4. Have there been significant changes in the makeup of management or the board of directors?

5. Has there been a high turnover of management and/or board members?

**Understanding What Motivates Management and the Board of Directors**

1. Is the personal worth of any of the key executives tied up in the organization?

2. Is management under pressure to meet earnings or other financial expectations, or does management commit to analysts, creditors, and others to achieve what appear to be unduly aggressive forecasts?

3. Is management's compensation primarily performance-based (bonuses, stock options, etc.)?

4. Are there significant debt covenants or other financial restrictions that management must meet?

5. Is the job security of any key members of management at serious risk?

**Understanding the Degree of Influence of Key Members of Management and/or the Board of Directors**

1. Who are the key members of management and the board of directors who have the most influence?

2. Do one or two key people have a dominant influence in the organization?

3. Is the management style of the organization more autocratic or democratic?

4. Is the organization's management centralized or decentralized?

5. Does management use ineffective means of communicating and supporting the entity's values or ethics, or do they communicate inappropriate values or ethics?

## Relationships with Others

Financial statement fraud is often perpetrated with the help of other real or fictitious organizations.

**Examples**

Enron's fraud was primarily conducted through what are known as special purpose entities (SPEs), which are business interests formed solely to accomplish some specific task or tasks. SPEs were not themselves illegal.

Lincoln Savings and Loan used relationships to commit fraud. In Lincoln's case, it structured sham transactions with certain straw buyers to make its negative performance appear profitable.

Although relationships with all parties should be examined to determine if they present management fraud opportunities or exposures, relationships with related organizations and individuals, external auditors, lawyers, investors, and regulators should always be carefully considered. Relationships with financial institutions and bondholders are also important because they indicate the extent to which the company is leveraged. Examples of the kinds of questions that should be asked about debt relationships include the following:

- Is the company highly leveraged, and with which financial institutions? What assets of the organization are pledged as collateral?
- Is there debt or other restrictive covenants that must be met?

- Do the banking relationships appear normal, or are there strange relationships with institutions, such as using institutions in unusual geographical locations?
- Are there relationships between the officers of the financial institutions and the client organization?

### *Relationships with Financial Institutions*

The real estate partnership referred to earlier involved a Wisconsin company taking out unauthorized loans from a bank located in another state, where it had no business purpose. The bank was used because the CEO of the client company had a relationship with the bank president, who later falsified an audit confirmation sent by the bank to the auditors. The loans were discovered when the auditors performed a lien search on properties owned. Because the bank president denied the existence of the loans, liabilities were significantly understated on the balance sheet.

1. With what financial institutions does the organization have significant relationships?

2. Is the organization highly leveraged through the bank or other loans?

3. Do any loan or debt covenants or restrictions pose significant problems for the organization?

4. Do the banking relationships appear normal, or are there unusual attributes present with the relationships (strange geographical locations, too many banks, etc.)?

5. Do members of management or the board have personal or other close relationships with officers of any of the major banks used by the company?

### *Relationships with Related Organizations and Individuals*

Related parties, which include related organizations and individuals such as family members, should be examined because structuring non-arm's length and often unrealistic transactions with related parties is one of the easiest ways to perpetrate financial statement fraud. These kinds of relationships are usually identified by examining large and/or unusual transactions, often occurring at strategic times (such as at the end of a period) to make the financial statements look better. The kinds of relationships and events that should be examined include the following:

- Large transactions that result in revenues or income for the organization
- Sales or purchases of assets between related entities
- Transactions that result in goodwill or other intangible assets being recognized in the financial statements
- Transactions that generate non-operating, rather than operating, income
- Loans or other financing transactions between related entities
- Any transaction that appears to be unusual or questionable for the organization, especially transactions that are unrealistically large

### *Relationship with Auditors*

The relationship between a company and its auditors is important to analyze for several reasons.

1. Have frequent disputes occurred with the current or predecessor auditors on accounting, auditing, or reporting matters?

2. Has management placed unreasonable demands on the auditor, including unreasonable time constraints?

3. Has the company placed formal or informal restrictions on the auditor that inappropriately limit his or her access to people or information or his or her ability to communicate effectively with the board of directors or the audit committee?

4. Does domineering management behavior characterize the dealings with the auditor, especially any attempts to influence the scope of the auditor's work?

5. Has an auditor change occurred? If so, for what reason?

6. Are any other relationships with the auditor questionable?

### *Relationship with Lawyers*

Relationships with lawyers pose even greater risks than relationships with auditors. While auditors are supposed to be independent and must resign if they suspect that financial results may not be appropriate, lawyers are usually advocates for their clients and will often follow and support their clients until it is obvious that fraud has occurred. In addition, lawyers usually have information about a client's legal difficulties, regulatory problems, and other significant occurrences. Like auditors, lawyers rarely give up a profitable client unless there is something obviously wrong. Thus, a change in legal firms without an obvious reason is often a cause for concern.

1. Has the company been involved in significant litigation concerning matters severely and adversely affect the company's financial results?

2. Has any attempt been made to hide litigation from the auditors or others?

3. Has any change occurred in outside counsels? If so, for what reasons?

4. Are any other lawyer relationships questionable?

### *Relationship with Investors*

Relationships with investors are important because financial statement fraud is often motivated by a debt or an equity offering to investors. In addition, knowledge of the number and kinds of investors (public vs. private, major exchange vs. small exchange, institutional vs. individual, etc.) can often indicate the degree of pressure and public scrutiny upon the management of the company and its financial performance.

If an organization is publicly held, investor groups or investment analysts usually follow the company very closely and can often provide information or indications that something is wrong with it.

 Example:

Some investors sell a company's stock "short," meaning they borrow shares from a brokerage and sell the shares at today's price with the intention to repay the borrowed stock they sold at some future time when the stock is trading for a lower price. These "short" sellers are always looking for bad news about an organization that will make its stock go down. If they suspect that something is not right, they will often publicly vent their concerns.

1. Is the organization in the process of issuing an initial or secondary public debt or equity offering?

2. Are any investor-related lawsuits pending or ongoing?

3. Are any relationships with investment bankers, stock analysts, or others problematic or questionable?

4. Has significant "short selling" of the company's stock occurred? If so, for what reasons?

5. Are any investor relationships questionable?

### *Relationship with Regulatory Bodies*

1. Does management display a significant disregard for regulatory authorities?

2. Has there been a history of securities law violations or claims against the entity or its senior management alleging fraud or violations of securities laws?

3. Have any 8-Ks been filed with the SEC? If so, for what reasons?

4. Could any new accounting, statutory, or regulatory requirements impair the financial stability or profitability of the entity?

5. Are significant tax disputes with the IRS or other taxing authorities pending?

6. Is the company current on paying its payroll taxes and other payroll-related expenses? Is the company current on paying other liabilities?

7. Are any other relationships with regulatory bodies questionable?

### Organization and Industry

Financial statement fraud is sometimes masked by creating an organizational structure that makes it easy to hide fraud. The kinds of questions that should be asked to understand the exposure to management fraud are as follows:

1. Does the company have an overly complex organizational structure involving numerous or unusual legal entities, managerial lines of authority, or contractual arrangements without apparent business purpose?

2. Is a legitimate business purpose apparent for each separate entity of the business?

3. Is the board of directors comprised primarily of officers of the company or other related individuals?

4. Is the board of directors passive or active and independent?

5. Is the audit committee comprised primarily of insiders or outsiders?

6. Is the audit committee passive or active and independent?

7. Does the organization have an independent or active internal audit department?

8. Does the organization have offshore activities without any apparent business purpose?

9. Is the organization a new entity without a proven history?

10. Have significant recent changes occurred in the nature of the organization?

11. Is monitoring of significant controls adequate?

12. Are the accounting and information technology staff and organization effective?

13. Is the degree of competition or market saturation high, accompanied by declining margins?

14. Is the client in a declining industry with increasing business failures and significant declines in customer demand?

15. Are changes in the industry rapid, such as high vulnerability to quickly changing technology or rapid product obsolescence?

16. Is the performance of the company similar or contrary to other firms in the industry?

17. Are there any other significant issues related to the organization and industry?

### Financial Results and Operating Characteristics

Much can be learned about exposure to financial statement fraud by closely examining management and the board of directors, relationships with others, and the nature of the organization. Looking at those three elements usually involves the same procedures for all kinds of financial statement frauds, whether the accounts manipulated are revenue accounts, asset accounts, liabilities, expenses, or equities.The kinds of exposures identified by the financial statements and operating characteristics of the organization differ from fraud scheme to fraud scheme. In examining financial statements to assess fraud exposures, a nontraditional approach to the financial statements must be taken.

Fraud symptoms most often exhibit themselves through changes in the financial statement. For example, financial statements that contain large changes in account balances from period to period are more likely to contain fraud than financial statements that exhibit only small incremental changes in account balances.

A sudden, dramatic increase in receivables, for example, is often a signal that something is wrong.

In addition to changes in financial statement balances and amounts, understanding what the footnotes are really saying is very important. Many times, the footnotes strongly hint that fraud is occurring; but what is contained in the footnotes is not clearly understood by auditors and others.In assessing fraud exposure through financial statements and operating characteristics, the balances and amounts must be compared with those of similar organizations in the same industry, and the real-world referents to the financial statement amounts must be determined.

Using financial relationships to assess fraud exposures requires that you know the nature of the client's business, the kinds of accounts that should be included, the kinds of fraud that could occur in the organization, and the kinds of symptoms those frauds would generate.In addition to considering the pattern of financial relationships, nonfinancial performance measures are also

valuable for detecting unusual financial results. Nonfinancial performance has been discussed in management accounting circles as a best practice for managing a business.

Some of the critical questions that must be asked about financial statement relationships and operating results are as follows:

1. Are unrealistic changes or increases present in financial statement account balances?

2. Are the account balances realistic given the nature, age, and size of the company?

3. Do actual physical assets exist in the amounts and values indicated on the financial statements?

4. Have there been significant changes in the nature of the organization's revenues or expenses?

5. Do one or a few large transactions account for a significant portion of any account balance or amount?

6. Are significant transactions made near the end of the period that positively impactsthe results of operations, especially transactions that are unusual or highly complex or that pose "substance over form" questions?

7. Do financial results appear consistent on a quarter-by-quarter or month-by-month basis, or are unrealistic amounts occurring in a subperiod?

8. Does the entity show an inability to generate cash flows from operations while reporting earnings and earnings growth?

9. Is significant pressure felt to obtain additional capital necessary to stay competitive, considering the financial position of the entity-including the need for funds to finance major research and development or capital expenditures?

10. Are reported assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties or that are subject to the potential significant change in the near term in a manner that may have a financially disruptive effect on the entity (i.e., ultimate collectibility of receivables, the timing of revenue recognition, realizability of financial instruments based on the highly subjective valuation of collateral or difficult-to-assess repayment sources, or significant deferral of costs)?

11. Does growth or profitability appear rapid, especially compared with that of other companies in the same industry?

12. Is the organization highly vulnerable to changes in interest rates?

13. Are unrealistically aggressive sales or profitability incentive programs in place?

14. Is a threat of imminent bankruptcy, foreclosure, or hostile takeover pertinent?

15. Are adverse consequences on significant pending transactions possible, such as a business combination or contract award, if poor financial results are reported?

16. Has management personally guaranteed significant debts of the entity when its financial position is poor or deteriorating?

17. Does the firm continuously operate on a "crisis" basis or without a careful budgeting and planning process?

18. Does the organization have difficulty collecting receivables or have other cash flow problems?

19. Is the organization dependent on one or two key products or services, especially products or services that can become quickly obsolete or where other organizations can adapt more quickly to market swings?

20. Do the footnotes contain information about difficult-to-understand issues?

21. Are adequate disclosures made in the footnotes?

22. Are financial results or operating characteristics accompanied by questionable or suspicious factors?

23. Are financial results consistent with nonfinancial performance indicators?

## Summary

Cases of financial statement fraud often have elements that are similar to the Phar-Mor fraud. First, the company appears to outperform others in the industry, and investors, analysts, or owners expect the company to perform at a very high level. At some point, the expectations of investors, analysts, or others will not be met, so pressure builds to do something to meet the high expectations. This is a turning point where fraud perpetrators step onto a slippery slope and slide down a mountain of deceit that is very difficult to reverse.

The person stepping onto the slippery slope is the manager or officer over financial reporting who agrees to violate an accounting principle and/or rule. The initial violation is often small compared to the fraud that is eventually detected. Sometimes the individual can rationalize that he or she is simply using his or her knowledge of accounting to "manage earnings" in a way that is beneficial for the company and investors. Almost always, the initial violation is viewed as aggressive but not fraudulent and is accompanied by an expectation that it will be a "one-time" event that will be corrected when operating performance improves in the future.

At this point, the officer over financial reporting has gained a reputation as the source of earnings when operations fall short. Because of the difficulty to resist this tremendous pressure when operations fall short in the future, the manager who committed a small, one-time fraud becomes the main source of earnings- fraudulent accounting practices. At this point, the fraud grows into a monster that needs constant care and attention. This growth process has been referred to as "a trickle to a waterfall," and it is often only a few short years before this seemingly innocent case of "earnings management" grows into a flood that ends up causing a financial and economic disaster by the time it is detected

## Keywords

Asset misappropriation: It is the theft that is committed by stealing receipts, stealing assets on hand, or committing some type of disbursement fraud.

Auditor: An auditor is a person authorized to review and verify the accuracy of financial records and ensure that companies comply with tax laws.

Embezzlement: It is the theft or fraudulent appropriation of money through deception.

Fictitious expense: A fictitious expense is where an employee invents an expense and then requests reimbursement for it. This can include receipts from companies that provide fake or novelty receipts.

Fictitious revenues: Fictitious revenues are created when an employee rings or enters a false sale into the company's accounting system or register. Many times fictitious revenues are created in Payroll Commission Schemes to increase the sales representatives' commission. The employer believes the sale to be legitimate and issues a commission check to the salesperson.

Financial Statement Fraud: Financial statement fraud is the deliberate misrepresentation of a company's financial statements, whether through omission or exaggeration, to create a more positive impression of the company's financial position, performance and cash flow.

Shell Company: A shell company is a fake entity that is solely created to bill a company for goods or services it does not receive.

Timing Difference: A timing difference occurs when the calculation of net income for accounting purposes varies from that determined for income tax purposes. Timing differences are temporary and journal entries are used to reverse the difference over time.

White Collar Crime: A crime committed by a person of respectability and high social status in the course of his occupation.

## Self Assessment

1. Identify the schemes involved in Rite Aid fraud.

A. Fabrication of Minutes by the CEO
B. Failing to Disclose the Related party transactions
C. Accounting Fraud Charges
D. Accounting Fraud Charges, Fabrication of Minutes by the CEO and Failing to Disclose the Related party transactions

2. Identify the schemes that Rite Aid used to inflate its profits:

A. Stock Depreciation Rights
B. Passing entries for Actual Expenses
C. Vendor Rebates
D. Overstating Inventory

3. Identify the schemes that Rite Aid did not use to inflate its profits:

A. Dead Deal
B. Will-Call Payables
C. Inventory Shrink
D. Disclosed Markdowns

4. Misleading financial statements results in _____.

A. Large losses to investors
B. Large profits to investors
C. Boosting trust in accounting systems
D. Decrease in litigation and embarrassment

5. Tyco scandal is an example of which of the following abuses?

A. Misstated financial statements and "cooking the books"
B. Inappropriate executive loans and corporate looting
C. Insider trading scandals
D. Excess CEO retirement perks

6. Martha Stewart is an example of which of the following abuses?

A. Insider trading scandals
B. Excess CEO retirement perks
C. Spinning and laddering
D. Loans for trading fees

7. In the Phar-Mor fraud case, several different methods were used for manipulating financial statements. These included all of the following except:

A. Overstating inventory
B. Recognizing revenue that should have been deferred
C. Funnelling losses into unaudited subsidiaries
D. Manipulating accounts

8. How many elements/factors are assumed to create the perfect fraud storm?

A. Five
B. Six
C. Seven
D. Nine

9. Management fraud is usually committed on behalf of the organization rather than against it. Which of the following would not be a motivation of fraud on behalf of an organization?

A. CEO needs a new car
B. A highly competitive industry
C. Pressure to meet expected earnings
D. Restructure debt covenants that can't be met

10. Correctly identifying exposures means that you must clearly understand :

A. the nature, structure and management of the organization
B. the nature of the industry and competition of the organization
C. relation of the organization with other parties and the influence that each of those parties has on management
D. all

11. Which of the following is not considered part of the fraud exposure rectangle?

A. Relationship with other
B. Management and Directors
C. Motivations for fraud
D. Financial Results and Operating Characteristics

12. The three aspects of management that a fraud examiner needs to be aware of include all of the following except:

A. Their backgrounds
B. Their motivations
C. Their religious convictions
D. Their influence in making decisions for the organization

13. One of the critical questions that must be asked about financial statement relationships and the operating results is:

A. Do actual physical assets exist in the amounts and values indicated on the financial statements?
B. Are the accounting and information technology staff and organization effective?
C. Is the degree of competition or market saturation high, accompanied by declining margins?
D. Is the client in a declining industry with increasing business failures and significant declines in customer demand?

14. The following question should be asked to understand the exposure to management fraud:

A. Is the company current on paying its payroll taxes and other payroll-related expenses? Is the company current on paying other liabilities?
B. Is the board of directors passive or active and independent?

C. Are the account balances realistic given the nature, age, and size of the company?

D. Do actual physical assets exist in the amounts and values indicated on the financial statements?

15. The following question should be asked to understand the relationship of an organization with Regulatory Bodies.

A. Does management display a significant disregard for regulatory authorities?

B. Are the account balances realistic given the nature, age, and size of the company?

C. Is the degree of competition or market saturation high, accompanied by declining margins?

D. Are any relationships with investment bankers, stock analysts, or others problematic or questionable?

## Answers for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | D | 2 | C | 3 | D | 4 | A | 5 | B |
| 6 | A | 7 | C | 8 | D | 9 | A | 10 | D |
| 11 | C | 12 | C | 13 | A | 14 | B | 15 | A |

## Review Questions

1. What were the schemes that Rite Aid used to inflate its profits?

2. List the most notable abuses that occurred in past two decades?

3. Explain the nine factors that led to the "perfect fraud storm." Illustrate how these factors helped create and foster ethical compromises.

4. What is financial statement fraud?

5. Who usually commits financial statement fraud?

6. What are common ways in which financial statement frauds are concealed?

7. How can an active audit committee help to deter financial statement fraud in an organization?

8. Explain some common motivations for financial statement fraud?

9. Explain the four different exposure areas that must be examined while detecting financial statement fraud?

10. Why must members of management and the board of directors be examined when searching for financial statement fraud exposures?

11. Why must relationships with others be examined when searching for financial statement fraud exposures?

12. When looking for financial statement fraud, why is it important to analyze the relationship between a company and its auditors?

## Further Readings

Pedneault, S., Rudewicz, F., Sheetz, M., & Silverstone, H. (2012). *Forensic Accounting and Fraud Investigation* (CPE ed.). John Wiley & Sons.

### Web Links

https://businessfraudprevention.org/glossary-of-fraud-terms/

# Unit 08: Income Statement Fraud

CONTENTS



## Objectives

After studying this unit, you will be able to:

- identify revenue-related financial statement fraud schemes.
- examine revenue-related financial statement fraud symptoms.
- summarize ways to actively search for symptoms of revenue-related financial statement fraud.
- identify Inventory-Related Fraud exposures.
- examine Inventory-Related Fraud Symptoms.
- summarize ways to actively search for symptoms of Inventory and Cost of Goods sold-related fraud.

## Introduction

A company can falsify its financial statements by implementing creative accounting practices, most common being inventory manipulation, revenue recognition frauds, malicious mergers or acquisitions, incorrect capitalisation of expenses and so on.

Revenue recognition fraud and inventory manipulation have been a major focus, revenue is a large part of financial statements thus it becomes a primary category that affects an entity's financial position and results of operations. The manipulation of revenue could result in a misstatement of an entity's EBITDA (Earnings before interest, tax, depreciation and amortization) and other profitability ratios, which investors and the public rely on when making investment decisions. Reliance on fraudulent information could eventually misstate the share price.

Inventory fraud involves the theft of physical inventory items and the misstatement of inventory records on a company's financial statements. Several high-profile financial statement frauds have involved the overstatement of inventory. This unit discusses revenue-related and inventory-related frauds, their symptoms and the mechanism to actively search for those symptoms.

## 8.1 Revenue-Related Fraud

The most common accounts manipulated when perpetrating financial statement fraud are revenues and/or receivables.

Over half of all financial statement frauds involved revenues and/or accounts receivable accounts (COSO-sponsored research).

Recording fictitious revenues and recording revenues prematurely are most common types of revenue related financial statement fraud. There are two reasons for the prevalence of revenue-related financial statement fraud. One is the availability of acceptable alternatives for recognizing revenue, and the other is the ease of manipulating net income using revenue and receivable accounts.

### Acceptable Alternatives

Just as organizations are different, the kinds of revenues they generate are different, and these different types of revenues need different recognition and reporting methods and criteria. A company that collects cash before delivering goods or performing a service, such as a franchiser, needs to recognize revenue differently than a company that collects cash after the delivery of goods or the performance of a service, such as a manufacturer. In many cases, it is difficult to identify one event that should trigger the recording of revenue.

**Example:**

A company that explores, refines, and distributes oil. When should revenue be recognized for this company-when it discovers the oil in the ground (for which there is a ready market and a determinable price), when it refines the crude oil or condensate into products such as jet and diesel fuel, when it distributes the oil to its service stations for resale, or when it actually sells the refined oil to customers?

These differences in revenue-recognition and performance criteria across organizations make it very difficult to develop revenue-recognition rules for the numerous business models in today's economy. Indeed, in many situations, significant judgment must be exercised to determine when and how much revenue to recognize. This provides opportunities for managers who want to commit financial statement fraud.

### Ease of Manipulating Net Income Using Revenues and Receivables

The second reason why revenue-related frauds are so common is because it is so easy to manipulate net income using revenues and receivables accounts. In the video Cooking the Books, produced by the Association of Certified Fraud Examiners, Barry Minkow, mastermind of the ZZZZ Best fraud, states, "Receivables are a wonderful thing. You create a receivable and you have revenue." When you have revenue, you have income. An easy way to inflate net income is to create revenue and some corresponding receivables. Additionally, revenues and receivables can be manipulated in several other ways.

**Example:**

An organization can inflate its revenues by including revenues in the current period that should be recognized in the next period. This scheme is often referred to as early or premature revenue recognition or abusing the cutoff.

Revenues can also be recognized early by misstating the work completed in a company with long-term construction contracts where revenue depends on a project's percentage of completion. Companies can also create fictitious documents, sales, or customers to make it appear that actual sales were higher than they really were for the period. Alternatively, contracts upon which revenue is based can be altered or forged. Or, in the most egregious cases, topside journal entries that create revenues and receivables without underlying documentation can be created.

### Identifying Revenue-Related Fraud Exposures

Revenue-related fraud exposures should be considered in every business. The exposures involve any schemes that can be used to misstate revenue and often misstate receivables, too. One of the best ways to understand how revenue frauds could be perpetrated is to understand the various revenue transactions in the company. One of the first tasks in this regard is to analyze and diagram the various transactions between an organization and its customers. Then, by analyzing the accounts involved in each transaction, an investigator or auditor can determine how each transaction could be misstated. Before, we discuss the various revenue-related fraud schemes, Let's list and briefly explain some of the more common ones. The following is a list of common revenue-related fraud schemes:

**Related-party transactions**are business deals or arrangements that are made by two parties who have a relationship (e.g., familial, business-related, or other) that creates conflicts of interest in a business setting. When related-party transactions are not disclosed, then fraud occurs.

**Sham sales**is a term used for various types of fictitious sales.

**Bill-and-hold sales**are orders for goods that are stored by the seller, often because the buyer is not ready or able to receive the goods at the time of the order. Fraud occurs when these sales are recognized even though the many requirements for their recognition (e.g., risk of loss must transfer to the buyer) are not.

**Side agreements**are sales terms and arrangements (e.g., a liberal return policy) that are made outside normal reporting channels. These agreements lead to fraud when theyinvolve amending the terms and conditions of existing sales contracts so that they violate revenue-recognition requirements.

**Consignment sales**are transactions where one company holds and sells goods that areowned by another company. Recording the full amount of a consignment sale leads to inflated revenues and corresponding costs.

**Channel stuffing**is a practice that suppliers use to encourage customers to buy extra inventory so as to increase current-year sales. This practice can inflate sales when stated or implied side agreements (e.g., allowing customers to return the goods) are not properlydisclosed or accounted for.

**Lapping or kiting**is a practice where cash receipts are misapplied to hide fictitious receivables. For example, if a fictitious receivable is recorded for Customer X, a received from Customer A will be used to show that the receivable was valid. A later payment received from another customer may be used to write off the receivable recordedby Customer A, etc. .

**Redating or refreshing transactions**involve changing sale dates to more current time periods to prevent them from being deemed uncollectible or bad debts.

**Liberal return policies**allow customers to return products and cancel sales in future periods. These policies make it difficult to estimate the amount of revenue that should be recorded in the current period.

**Partial shipment schemes**involve recording the full amount of a sale when only part of the sale was shipped.

**Improper cutoff**occurs when transactions are recorded in the wrong time period. This occurs when a company keeps the accounting books open for a particular period and records future-period transactions as if they occurred in the current period (also referred to as improperly holding the books open).

**Round-tripping**involves selling unused assets for a promise to buy them or similar assets back at roughly the same price. In the end, no economic benefit exists for either company.

All of these fraud schemes result in overstated revenues and over stated net income. Of course, it would also be possible to understate revenues and net income by committing fraud in the opposite direction. Such frauds are extremely rare and usually only occur when a company wants to manage or smooth income or understate net income in order to pay lower income taxes.

Let's discuss various transaction types that are used in various Fraud Schemes through the following Table

| Transaction | Accounts Involved | Fraud Scheme |
|---|---|---|
| 1. Sell goods and/or services to customers | Accounts Receivable and Revenues (e.g., Sales Revenue) | 1. Record fictitious sales (e.g., related parties. sham sales, bill-and-hold sales, sales with side agreements, consignment sales. round-tripping, etc.)<br>2. Recognize revenues too early (e.g., improper cutoff, holding books open after the close of a reporting period. |

| | | |
|---|---|---|
| | | percentage of completion, etc.)<br>3. Overstate real sales (e.g., use) improper valuation of revenue, alter contracts, inflate amounts, etc.) |
| 2. Estimate uncollectible receivables | Bad Debt Expense and Allowance for Doubtful Accounts | 4 Understate allowance for doubtful accounts, thus overstating receivables |
| 3. Accept returned goods from customers | Sales Returns and Accounts Receivable | 5. Not record returned goods from customers<br>6. Record returned goods after the end of the period |
| 4. Write off receivables as uncollectible | Allowance for Doubtful Accounts and Accounts Receivable | 7. Don't write off uncollectible receivables (e.g., redating)<br>8. Write off uncollectible receivables in a later period |
| 5. Collect cash after discount period | Cash and Accounts Receivable | 9. Record bank transfers as cash is received from customers<br>10. Manipulate cash received from related parties (e.g., lapping)<br>11. Record fictitious cash entries such as debiting Cash and crediting Accounts. Receivable |
| 6. Collect cash within discount period | Cash, Sales Discounts, and Accounts Receivable | 12. Not record discounts given to customers |

Once the various fraud schemes (or exposures) have been considered. scheme-specific symptoms can be searched for proactively. Any observed symptoms can be investigated to determine if fraud exists.

### Identifying Revenue-Related Fraud Symptoms

Unlike murder or bank robbery, fraud is rarely observed Instead, only symptoms, indicators, or red flags are observed. To detect fraud, you must be able to identify something as being a symptom or red flag. Fraud symptoms (for all types of fraud) can be divided into six categories as follows:

**1.Analytical symptoms**:These economic events, accounting transactions, or financial and nonfinancial relationships are unusual.

- Revenue or sales that appear too high.
- Sales discounts that appear too low.
- Sales returns that appear too low.
- Bad debt expense that appears too low.
- Accounts receivable that appear too high or are increasing too fast.

**2. Accounting or documentary symptoms:**These discrepancies in the accounting records or system involve such things as missing documents, photocopies where originals should exist, ledgers that don't balance, unusual journal entries, or similar events.

- Unsupported or unauthorized revenue-related balances or transactions.

- Missing documents in the revenue cycle.
- Only photocopies of documents exist to support revenue transactions, when documents in original form should exist.
- Significant unexplained items on bank and other reconciliations.
- Revenue-related ledgers (sales, cash receipts, etc.) that do not balance.

**3. Lifestyle symptoms:**When people steal, they spend their ill-gotten gains. Perpetrators rarely save what they steal. Once the critical need is met that motivated the fraud, perpetrators start to improve their lifestyle. Although management fraud in smaller companies and other types of misappropriation are often motivated by lifestyle symptoms. these types of symptoms are usually not as apparent in financial statement fraud in large organizations since management is usually very well compensated by legitimate means.

- Major sales of company stock around earnings releases or other unusual dates.
- Significant bonuses tied to meet earnings forecasts.
- Executives' personal net worth tied up in company stock.

**4. Control symptoms:**These breakdowns in the control environment, accounting system, or internal control activities or procedures are often so egregious that they hint that a management override is taking place. Examples are an override or lack of segregation of duties when segregation should exist, a weak or missing audit committee, etc.

- Management override of significant internal control activities related to the revenue cycle.
- New, unusual, or large customers that appear not to have gone through the customer-approval process.
- Weaknesses in the cutoff processes or other key accounting processes.

**5.Behavioral and verbal symptoms:**Most fraud perpetrators are first-time offenders. When they commit fraud, they feel guilty, which creates stress. Fraud perpetrators change their behavior to cope with this stress or to hide fraud symptoms. These changes in behavior, together with verbal responses, are often excellent fraud symptoms.

- Inconsistent, vague, or implausible responses from management or employees arising from revenue inquiries or analytical procedures.
- Denied access to facilities, employees, records, customers, vendors, or others from where revenue-related audit evidence might be sought.
- Undue time pressures imposed by management to resolve contentious or complex revenue related issues.
- Unusual delays by the entity in providing revenue-related, requested information.

**6. Tips and complaints:** The last category of fraud symptoms is tips or complaints from employees, spouses, vendors, customers, and others. Although no up should be ignored, many tips and complaints are motivated by nonfactors, such as revenge, attention seeking, or other reasons.

- Tips or complaints that revenue-related fraud (any of the schemes discussed) might be occurring, either from the company whistle-blower system or in other ways.
- Revenue frauds disclosed at companies with which this company does significant amount of business.

## Actively Searching for Revenue-related Analytical Symptoms

Analytical symptoms relating to revenue accounts involve those accounts being too high or too low, increasing too fast or not fast enough, or other abnormal relationships. When searching for analytical symptoms, the question that needs answering is "too high, too low, or unusual relative to what? To determine whether analytical symptoms exist, a point of reference, an expectation, or some reasonable balance or relationship to which recorded amounts can be compared is necessary. A practical way to begin looking for analytical symptoms is to focus on changes and

comparisonswithin the financial statements. The specific analyses that are conducted usually include the following:

1. Analyzing financial balances and relationships within financial statements.

2. Comparing financial statement amounts or relationships with other things.

Two common ways for performing a within statement analysis include looking for unusual changes in revenue-related (1) account balances from period to period (looking at trends) and (2) relationships from period to period. Two types of analyses can also be performed where financial statement amounts and relationships are compared to other information. These include the following:

1. Comparing financial results and trends of the company with those of similar firms in thesame industry or with industry averages.

2. Comparing recorded revenue in the financial statements with assets or other financial ornonfinancial information.

Let's summarizes these approaches of types of Financial Statement Analysis through the following table.

| | | |
|---|---|---|
| Analyzing financial balances and relationships within financial statements | Look for unusual changes in revenues and accounts receivable balances from period to period (trends) | Look for unusual changes in revenue- cycle-account relationships from period to period. |
| Comparing financial statement amounts or relationships with related information | Compare financial results and trends of the company with those of similar firm in the same industry. | Compare recorded amounts in the financial statements with financial or nonfinancial amounts. |

### Focusing on Changes in Recorded Account Balances (Amounts) from Period to Period

Recorded amounts from one period can be compared to recorded amounts in another period in three ways. The first and least effective method is to focus on and calculate changes in the actual financial statement numbers themselves. It is often difficult, however, to assess the magnitude or significance of changes in account balances looking only at raw data, especially when the numbers are large.

The second method, and one where it is much easier to recognize analytical symptoms, is to use a process described earlier in Chapter 6, called horizontal analysis. Horizontal analysis is a method involving examining percentage changes in account balances from period to period. The third way to examine changes from period to period is to study the statement of cash flows.

Perhaps you are wondering why we perform horizontal analysis only on the income statement and balance sheet, but not on the statement of cash flows. The reason is because horizontal analysis converts income statements and balance sheets to "change" statements, and the statement of cash flows is already a "change statement." Every number on the statement of cash flows represents the change in account balances from one period to the next.

### Focusing on Changes in Revenue-Related Relationships

Examining changes in financial statement relationships from period to period is one of the best ways to discover analytical fraud symptoms. Changes in relationships from period to period can be examined in at least two ways. The first is to focus on changes in various revenue- related ratios from period to period. (Ratios, as you will recall, are summary calculations of an efficient method of focusing on relationship symptoms within the financial statements. The significant relationships in the financial statements.) Examining revenue-related ratios provides most common ratios used to discover revenue-related analytical fraud symptoms are the following:

- Gross Profit Margin ratio
- Sales return percentage ratio
- Sales discount percentage ratio

- Accounts receivable turnover
- Number of days in receivables ratio
- Allowance for uncollectible accounts as a percentage of receivables
- Asset turnover ratio
- Working capital turnover ratio
- Operating performance margin ratio
- Earnings per share

Adding fictitious receivables will generally increase the number of days it takes to collect receivables because none of the fictitious receivables will be collected.

When using ratios to discover financial statement fraud symptoms, remember that the size or direction of the ratio is usually not important; rather, the changes (and speed of changes) in the ratios are what signal possible fraud-especially when the change is unexpected or unexplained.

The second way to focus on financial statement relationships as fraud symptoms is to convert the financial statements to percentages and perform vertical analysis.Vertical analysis is effective for identifying changes in financial statement relationships that must be investigated. With ratios, you generally focus on only one or two financial statement relationships at a time. If that relationship turns out to be the best indicator of fraud, you may identify a fraud symptom. On the other hand, with vertical analysis, you can simultaneously view the relationships between all numbers on the balance sheet or income statement.

The difficulty in using horizontal, vertical, or ratio analysis is knowing when a change in account balance or relationship is significant enough to signal possible fraud. Developing a reliable expectation or prediction regarding what the ratio or relationship should look like is the most important step in this process. Experience with and knowledge about a company are necessary for developing a reliable expectation.

### Comparing Financial Statement Information Between Companies

One of the best ways to detect financial statement fraud is to compare the performance of the company you are examining with the performance of other similar companies in the industry.Performance that runs counter to the performance of other firms in the same industry often signals fraud.

In the Equity Funding fraud, the financial statements showed a highly profitable and growing insurance company at a time when the rest of the insurance industry was struggling and significantly less profitable.

### Comparing Financial Statement Amounts with the Assets They Represent

Comparing recorded amounts in the financial statements with real-world assets is often anexcellent way to detect fraud. However, this approach is not as useful for detecting revenue- related frauds as it is for detecting cash, inventory, and physical asset frauds. Generally, revenues do not correspond to physical assets that can be examined. The exception is when a company earns revenue constructing assets that involve long-term construction projects such as a building, bridge, or highway and recognizes revenue on the percentage-of-completion method. In these cases, the constructed assets should be examined to determine if the revenue recognized is reasonable, given the degree of completion of the projects.

### Actively Searching for Accounting or Documentary Symptoms

One of the common ways for management to commit fraud is through posting one or more journal entries directly to the accounting records. These entries often bypass the normal process for posting journal entries and therefore involve the overriding of internal controls. These entries, are often referred to as "topside" journal entries, meaning the entries are posted directly to the summary journal or general ledger instead of a subsidiary ledger where supporting information is maintained.

In a sales related fraud scheme, management might post a topside journal entry to increase both sales and accounts receivable. Normally, when sales and accounts receivable increase, entries are made to subsidiary journals showing who purchased the goods or services, the date of the purchase, when it was shipped, and so forth. With a topside journal entry, this supporting information is not recorded, and the entry increases the accounts but not the supporting ledgers such as the sales journal or the accounts receivable ledger.

One of the challenges in analyzing millions of journal entries using an inductive method is that you will end up with hundreds, even thousands, of false positives (entries that look unusual but are not). Even so, this sort of analysis was the breakthrough that allowed the WorldCom internal auditors to detect the company's massive financial statement fraud.

### Actively Searching for Control Symptoms

The importance of identifying control weaknesses as possible fraud symptoms has already been discussed. However, two control- related points need mentioning with respect to revenue-related frauds. First, accountants and financial statement auditors are accustomed to accepting a limited number of control exceptions when assessing the adequacy of a system of internal controls. This approach is used because they view control breakdowns or weaknesses as something that needs to be fixed "in the future." As a fraud examiner, you must remember that most frauds are motivated by something called the fraud triangle.

The second control factor that deserves special attention in considering financial statement fraud is the control environment. In many cases of financial statement fraud, the audit committee or board of directors is weak or inactive, and one or two executives have controlling power in the organization. A weak audit committee or board can lead to a control environment that does not value ethical behavior and it increases the chances of committing fraud.

### Actively Searching for Behavioral or Verbal and Lifestyle Symptoms

With respect to behavioral symptoms, remember that committing fraud, especially for first-time offenders, creates stress. Perpetrators must find a way to cope with that stress, and they usually do so by changing their behavior. Although financial statement auditors and fraud examiners may not be familiar enough with the management of a company to recognize changes in behavior, others within the organization are. In these situations, asking questions of lots of people will often reveal that something is not right.

Fraud examiners and auditors should learn to ask key fraud-related questions, such as the following:

- Have you seen anything that resembles that something isn't right or that could be considered a red flag of fraud?
- Have you been asked to make any accounting entries that you consider to be unusual or about which you had questions regarding their propriety?
- Is there anything suspicious I should be aware of in this company?
- Have there been any attempts to manage earnings?
- Do any unusual operating or nonoperating income items concern you?
- Why did revenues (or returns, discounts, bad debts, allowances, etc.) change so dramatically?
- Should I pay particular attention to any specific individuals or units in the organization?
- What I part of this organization, or which individuals, keep you awake worrying at night?

### Actively Searching for Tips and Complaints

- The best way to search for tips and complaints for any fraud is to institute an ombudsman, hotline, or other system whereby people can anonymously call with tips and complaints.

- Implement whistle-blowing systems

### Following Up on Revenue-Related Fraud Symptoms

As a fraud examiner, the presence of fraud symptoms provides predication or reason to believe that fraud may be occurring. When predication exists, and if conditions warrant, an investigation should take place. In this case, various investigative procedures help to determine whether fraud is actually occurring and, if so, the extent of the fraud. The specific procedures used, and the specific procedures used, and the order in which they are used, depends on the kind of fraud you suspect and the ease of collecting evidence.

## 8.2 Inventory and Cost of Goods Sold Frauds

Besides revenue-related fraud schemes, the next most common financial statement fraud schemes involve the manipulation of inventory and cost of goods sold accounts. Several high-profile financial statement frauds have involved the overstatement of inventory.

Phar Mor significantly overstated the value of its inventory and then moved inventory back and forth between stores so that it could be counted multiple times.

To understand why inventory-related fraud schemes are so common, you should understand how inventory accounts affect the income statement.

Let's analyze the Effects of Inventory Overstatement on the Income Statement

| Income Statements | When inventory is overstated, them: |
|---|---|
| - Gross Revenues (Sales) | Are not affected |
| - Sales Returns | Are not affected |
| - Sales Discounts | Are not affected |
| Net Revenue (Sales) | Are not affected |
| - Cost of Goods Sold | Is understated |
| Gross Margin | Is overstated |
| - Expenses | Are not affected |
| Net Income | Is overstated |

From this analysis, you can see that if inventory is overstated, cost of goods sold is understated, and gross margin and net income are overstated by an equal amount (less the tax effect).

To better understand the effect of cost of goods sold on inventory, let's consider the calculations of Cos of goods sold through following table:

| Cost of Goods Sold Calculations | Period I, Overstatement of Ending Inventory | Period 2 |
|---|---|---|
| Beginning Inventory | Not affected | Overstated |
| + Purchases of Inventory | Not affected | Not affected |
| - Returns of Inventory to Vendor | Not affected | Not affected |
| - Purchase Discounts on Inventory Purchases | Not affected | Not affected |
| = Goods Available for Sale | Not affected | Overstated |
| - Ending Inventory | Overstated | Not affected |
| = Cost of Goods Sold | Understated | Overstated |

This analysis shows that the overstatement of ending inventory in period 1 has an effect on cost of goods sold in both periods 1 and 2. Furthermore, cost of goods sold can be understated by either understating purchases or overstating inventory.

It can also be understated by overstating purchase returns or purchase discounts. Of these alternatives, overstating the ending inventory tends to be the most common fraud because it increases net income and recorded assets, making the balance sheet look better.

The analysis above also illustrates why overstating inventory is a fraud that is very difficult to maintain without getting caught. In the first period, when ending inventory is overstated, cost of goods sold is understated, making gross margin and net income overstated.

However, that overstated ending inventory becomes the beginning inventory in period 2, meaning that further overstatements of ending inventory must be made or cost of goods sold in period 2 will be overstated and gross margin and net income will be understated.

This offsetting effect from one period to the next makes it necessary for offset the effect of his inventory in period 2 by an even larger amount in order to both offset the effect of having an overstated beginning inventory and to commit additional fraud. Perpetrators who are smart should commit other types of financial statement fraud other than overstating inventory because of the compounding effect from period to period.

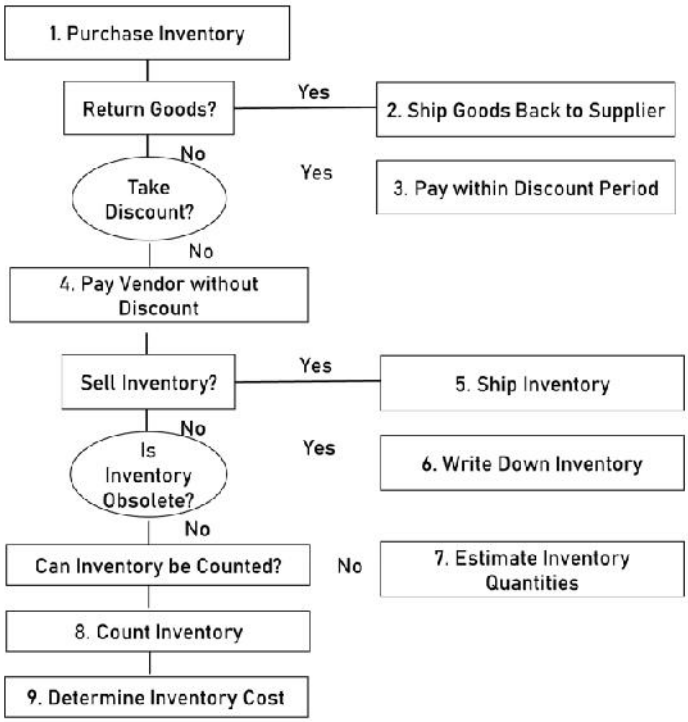
### Identifying Inventory-Related Fraud Exposures

To understand inventory-related financial statement frauds, we follow the same process we used to discuss revenue related frauds. That is, we first identify financial statement fraud exposures. Then we discuss inventory-related fraud symptoms. Third, we consider ways to actively search for fraud symptoms. Last, we cover ways to follow up on symptoms to discover inventory related frauds.

There are numerous potential inventory-related fraud schemes. Some of the most commonschemes include the following:

- Double Counting
- Capitalizing costs that should be expensed
- Cutoff problems
- Overestimating inventory
- Bill-and-hold sales
- Consigned inventory

As with revenue-related frauds, one of the best ways to identify financial statement fraud exposures is to diagram the various kinds of inventory-related transactions that can occur in an organization. For many companies, the inventory-related transactions might appear as shown inthe following Figure.




As you can see from the flowchart in the above Figure, nine different transactions affect the accounting for inventories and cost of goods sold. Now, let's see the accounts and the fraud schemes that could occur in each of these transactions.

| **Transactions** | **Accounts Involved** | **Fraud Scheme** |
|---|---|---|
| Purchase Inventory | Inventory, Accounts Payable | 1. Under-record purchases<br>2. Record purchases too late<br>3. Do not record purchases |
| Return merchandise to supplier | Accounts Payable, Inventory | 1. Overstate returns<br>2. Record returns in an earlier period (cutoff problem) |
| Pay vendor within discount period | Accounts Payable, Inventory, Cash | 1. Overstate discounts<br>2. Do not reduce inventory cost |
| Inventory is sold; COGS is recognized | COGS, Inventory | 1. Record at too low an amount<br>2. Do not record COGS or reduce inventory |
| Inventory becomes obsolete and is written down | Loss on Write-Down of Inventory, Inventory | Do not write off or write down obsolete inventory |

| | | |
|---|---|---|
| Inventory quantities are estimated | Inventory Shrinkage, Inventory | Overestimate inventory |
| Inventory quantities are counted | Inventory Shrinkage, Inventory | 1. Over count inventory (double counting, etc.)<br>2. Capitalize amounts that should be expensed |
| Inventory cost is determined | Inventory, COGS | 1. Use Incorrect costs<br>2. Make incorrect extensions<br>3. Record fictitious Inventory |

As you can see, by focusing on the various transactions and inventory counts, we have identified 16 fraud schemes that can be used to overstate inventory or understate cost of goods sold. Obviously, some of these schemes are more common than others, but all can be used to misstate inventory and cost of goods sold. As with revenues, all of these fraud schemes can be used to increase net income. Additionally, it is possible to commit inventory fraud by understating inventory and net income. However, this is a rare situation that may arise in a privately owned company that wants to decrease the amount of income taxes paid to the government. Because it is so rare, we ignore this situation in our discussion.

As stated earlier, inventory overstatement frauds are much more difficult for perpetrators than revenue frauds. With revenue-related frauds, reported revenues are overstated in the current period, and accounts receivable are overstated on the balance sheet. However, a reversing effect does not automatically occur in the subsequent period as it does with inventory. With inventory frauds, the "overstated ending inventory" of one period becomes the "overstated beginning inventory" of the next period and causes net income to be understated in the second period. Thus, if a dishonest management wanted to continue the fraud and overstate net income in a second period (most frauds are multiple-period frauds), it would have to perpetratea fraud of an equivalent magnitude just to offset the overstated beginning inventory and then commit an additional fraud if they again wanted to increase net income. The results are larger misstatements of inventory and a fraud that is much easier to detect. Fortunately, most financial statement frauds are perpetrated because of desperation. As such, & perpetrator generally worries only about how income can be overstated in the current period, with no thought of the problems it creates in subsequent periods.

### Identifying Inventory-Related Fraud Symptoms

Once again, we use the six categories of fraud symptoms to discuss inventory and cost of goods sold frauds. Some of the most common symptoms with these frauds are listed here. Rather than discuss them in detail as we did for revenue-related frauds, we will simply list them by category.

### Analytical Symptoms

- Reported inventory balances that appear too high or are increasing too fast.
- Reported cost of goods sold balances that appear too low or are decreasing too fast.
- Reported purchase returns that appear too high or are increasing too rapidly.
- Reported purchase discounts that appear too high or are increasing too rapidly.
- Reported purchases that appear too low for sales or inventory levels.
- Capitalized inventory that looks as if it should be expensed.

### Accounting or Documentary Symptoms

- Inventory or cost of goods sold transactions that are not recorded in a complete or timely improperly recorded as to amount, accounting period, classification, or entity.
- Unsupported or unauthorized inventory or cost of goods sold-related transactions.
- End-of-period inventory or cost of goods sold adjustments that significantly change the entity's financial results.
- Missing documents related to inventory and/or cost of goods sold.
- Unavailability of other than photocopied documents to support inventory or cost of goods sold transactions when original documents should exist.

### Control Symptoms

- Management override of significant internal control activities related to purchases, inventory, or cost of goods sold.
- New or unusual vendors that appear not to have gone through the regular vendor-approval process.
- Weaknesses in the inventory counting process.

### Behavioral or Verbal Symptoms

- Inconsistent, vague, or implausible responses from management or employees arising from inventory, purchase, or cost of goods sold-related inquiries or analytical procedures.
- Denied access to facilities, employees, records, customers, vendors, or others from whom inventory or cost of goods sold-related evidence might be sought.
- Undue time pressures imposed by management to resolve contentious or complex inventory or cost of goods sold-related issues.
- Unusual delays by the entity in providing requested inventory or cost of goods sold- related information.

### Lifestyle Symptoms

- Similar symptoms to the revenue-related frauds (e.g., stock sales, bonuses, and stock ownership). However, remember that lifestyle symptoms are often not very effective for detecting financial statement frauds.

### Tips and Complaints

Tips or complaints that come in through the whistle-blowing system or through othermeans may suggest that inventory-related fraud schemes might be occurring.

While these lists are not exhaustive, they represent some common inventory and cost of goods sold-related fraud symptoms that can be observed.

### Proactively Looking for Inventory-related Fraud Symptoms

Observing fraud symptoms is a key to detecting inventory-related financial statement frauds. Take the MiniScribe Corporation financial statement fraud.

Case: MiniScribe

MiniScribe's management, with the assistance of other officers and employees, engaged in a series of fraudulent activities that overstated inventory and materially inflated reported net income. Since MiniScribe fraudulently inflated its inventory using schemes

that reversed each period, there was a constant need to misstate larger and larger amounts, and the fraud grew rapidly. In the first year, the inventory overstatement was $4.5 million. In the second year, the overstatement was $22 million. In the third year (two quarters only), the overstatement was $31.8 million.

To understand the kinds of symptoms available, understanding how management perpetrated the fraud is necessary. In the first year, managers from MiniScribe broke into the auditors' files to find inventory lists that designated which items in inventory had been test-counted. With this information, the officers inflated the values of the inventory items that were not counted by the auditors. In the second year, with the need to misstate inventory by a much larger amount, management used the following three different approaches:

- Created fictitious "inventory in transit" amounts.
- Recorded a transfer of $9 million in nonexistent inventory from MiniScribe's U.S. books to the books of MiniScribe's Far East subsidiaries.
- Received raw materials into inventory just prior to the end of the fiscal year without recording the corresponding accounts payable liability.

In the third year, management resorted to even more egregious ways to overstate inventory. As an example of its desperate attempts to misstate inventory, it shipped boxes of bricks labeled as disk drives to two MiniScribe distributors and recorded the shipments as consigned inventory. Management even created a computer program called "Cook Book" to generate fictitious inventory numbers. It also accumulated scrap that had been written off the company's books, repackaged it, and added it to the accounting records as inventory. Employees of the company even prepared false inventory tickets to increase recorded inventory.

In the first year, the MiniScribe fraud would probably have been very difficult to detect. When management breaks into auditors' files, steals information, and forges computer records that are not test-counted by auditors, the fraud has little chance of being caught. Maybe management's behavior or responses to auditors' inquiries will change and possibly someone will provide a tip, but there are not many accounting, documentary, or control symptoms that can alert an auditor that fraud is occurring. Also, since the fraud in that first year was only $4.5 million, the analytical symptoms were not too significant.

In the second year, as the fraud grew to $22 million and took on different forms, more and more symptoms must have appeared. For example, the huge increase in the inventory balance was a glaring analytical symptom. Also, the large in-transit inventory amounts, especially at year-end, must have appeared unusual. Together with the $9 million transfer of inventory from the U.S. parent's books to an Asian subsidiary's books, these two transactions should have raised concerns. Certainly, inventory that is listed as an asset without a corresponding purchase creates an accounting symptom. With these kinds of suspicious year-end transactions, inquiries of management should increase, providing auditors and fraud examiners with an opportunity to observe the consistency of management's behavior and verbal responses. In the second year, some overriding of key controls and maybe even a tip or two were likely to appear as more and more people became knowledgeable about the fraud.

In the third year, when boxes of bricks were being shipped, consigned inventory increased, and a new fraudulent computer program was written, more and more symptoms had to surface. Returns of merchandise (bricks) and customer complaints were likely increasing. More and more employees were involved, leading to a higher probability of a tip or complaint, and false inventory tickets and the reclassification of obsolete inventory as good inventory had to be present.

Source: Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., &Zimbelman, M. (2009). *Forensic Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.

### Searching for Inventory and Cost of Goods Sold Analytical Symptoms

As with other types of fraud, inventory-related fraud symptoms can be found in one of the following two ways:

- Wait until you "happen on to them by chance."
- Proactively search for them.

The following table summarizes the for analyzing Financial Statements for Inventory Fraud

| | | |
|---|---|---|
| Analyzing financial balances and relationships within financial statements | Look for unusual changes in inventory and cost of goods sold account balances from period to period. | Look for unusual changes in inventory and cost of goods sold relationships from period to period. |
| Comparing financial statement amounts or relationships with other information | Compare financial results and trends of the company with those of similar firms in the same industry. | Compare recorded amounts in the financial statements with nonfinancialstatement amounts. |

### Focusing on Changes in Recorded Balances from Period to Period

Recall from our discussion of revenue-related frauds that there are three ways to focus onchanges in recorded balances from period to period. The first and usually least effective method is to focus on the changes in the actual financial statement numbers. Because financial statement inventory and cost of goods sold numbers are often large, it is often difficult, examining the numbers alone, to assess the magnitude of changes or to distinguish significant from insignificant changes. A second, similar method is to study the statement of cash flows. This statement identifies changes in account balances from one period to the next. The advantage of focusing on the statement of cash flows is that the "change" numbers have already been calculated.

Probably the best way to examine changes in account balances from period to period is to use horizontal analysis.

### Focusing on Changes in Relationships from Period to Period

As with revenue-related financial statement frauds, two primary methods can be used to focus on changes in relationships from period to period. The first is to examine ratio changes from one period to the next. The second is to convert the financial statements to common-size statements and use vertical analysis to examine the percentage changes from period to period.

The most helpful ratios used to examine inventory and cost of goods sold relationships are as follows:

Primary three ratios

- Gross profit (margin) ratio
- Inventory turnover ratio
- Number of days' sales in inventory

Secondary four ratios

- Asset turnover
- Working capital turnover
- Operating performance ratio and
- Earnings per share

The second way to focus on financial statement relationships is to convert the financial statements to common-size statements and perform vertical analysis.

### Comparing Financial Statement Information with Other Companies

Maintaining large amounts of inventory is quite expensive, especially if the inventory is large, bulky, heavy, or requires special handling. Because inventory handling and warehouse costs, as well as financing costs, are extremely expensive, most companies are taking major steps to decrease the inventory they have on hand. For example, Dell Computer keeps very little inventory on hand

and purchases its inventory just in time to assemble computers already ordered by its customers. Investors often see large amounts of inventory as a sign of inefficiency in a company's operations. Therefore, in most cases, when a company's reported inventory balance increases, you should ask why.

Increasing amounts of inventory are especially questionable when other companies against which a company competes are not increasing their inventory balances. Increased inventories can represent poor management decisions, fraud, or increased sales expectations, which if not realized, can cause significant losses for the company.

In comparing inventory balances and trends with similar companies, the type of inventory a company has should be considered.

### Comparing Financial Statement Amounts with the Assets they Represent

Comparing recorded amounts in the financial statements with the assets they are supposed to represent is an excellent way to detect inventory-related financial statement frauds. In a fraud perpetrated by Laribee Wire Manufacturing Co., the inventory represented by the financial statement amounts would have required three times the capacity of the buildings the company had in which to store it.

### Actively Searching for Accounting or Documentary Symptoms

As with revenue-related frauds, a common way for management to commit an inventory- related fraud is by posting topside journal entries to the accounting records. Software such as ACL or IDEA can be used to determine if any journal entries are unusual in terms of the five Ws: (1) who posted the entry, (2) what the entry was for, (3) when the entry was posted, (4) where the entry was posted in the accounting system, and (5) why the entry was posted.

### Actively Searching for Inventory-Related Control Symptoms

Because inventory frauds, like revenue-related frauds, are so prevalent, a good control environment and control procedures should be in place.

Inventory controls must be examined closely. Remember that the lack of a key control provides a fraud opportunity that completes the fraud triangle.

Where inventory controls are weak or easily overridden, a missing control or an observance of an override represents a fraud symptom, not just a control weakness. As such, it should be pursued with the same vigilance as any other fraud symptom.

### Actively Searching for Behavioral or Verbal and Lifestyle Symptoms

As with other financial statement frauds, lifestyle symptoms are usually not very effective in helping you find inventory-related financial statement fraud because financial statement fraud usually does not benefit the perpetrators directly. However, searching for behavioral and verbal symptoms can be very fruitful. Often, recorded inventory amounts are subject to management's intent. Usually, the best evidence relating to management's intent is interviewing or inquiry.

### Actively Searching for Tips and Complaints

Tips and complaints are fruitful areas for detecting inventory-related frauds. In most cases. because of its physical characteristics, inventory must be brought into a firm, handled within the firm, and shipped when sold. All this movement means that people must be involved in managing and handling the physical flow of inventory. Usually, these individuals do not understand the nature of audits or forensic examinations, nor the kinds of fraud that could be occurring.

In addition to individuals who handle the inventory, it is often helpful to communicate directly with vendors to determine their relationships with the company. Although you have to be careful not to intrude in the company's business and hurt its relationships with vendors, you can often learn valuable information about inventory costs, amounts of purchases, and other factors by speaking with those vendors. Similarly, talking with large customers and assessing inventory quality and product returns will often provide evidence.

## Summary

The most common accounts manipulated when perpetrating financial statement fraud are revenues and/or receivables.

Recording fictitious revenues and recording revenues prematurely are most common types of revenue related financial statement fraud. There are two reasons for the prevalence of revenue-related financial statement fraud. One is the availability of acceptable alternatives for recognizing revenue, and the other is the ease of manipulating net income using revenue and receivable accounts.

One of the best ways to understand how revenue frauds could be perpetrated is to understand the various revenue transactions in the company.

Fraud symptoms (for all types of fraud) can be divided into six categories namely Analytical symptoms, Accounting or documentary symptoms, Lifestyle symptoms, Control symptoms, Behavioral and verbal symptoms and Tips and complaints.

Besides revenue-related fraud schemes, the next most common financial statement fraud schemes involve the manipulation of inventory and cost of goods sold accounts.

Several high-profile financial statement frauds have involved the overstatement of inventory. For example Phar Mor scam.

If inventory is overstated, cost of goods sold is understated, and gross margin and net income are overstated by an equal amount (less the tax effect).

Overstating the ending inventory tends to be the most common fraud because it increases net income and recorded assets, making the balance sheet look better.

Inventory overstatement frauds are much more difficult for perpetrators than revenue frauds.

## Keywords

Asset turnover ratio: It is most helpful in detecting fraud when inventory comprises a large percentage of an organization's assets. It is calculated by dividing net sales by average total assets.

Consigned inventory: These are goods that the company holds and sells for another company. Because the company holding the goods does not own them, it may inflate ending inventory by including the consigned inventory in its year-end physical count.

Cutoff problems: It occur when a company delays the write-down of obsolete inventory, records returns from an earlier period, records purchases in a later period, and performs other such practices.

Double counting: It occurs when specific inventory items are counted twice. This may be due to a company moving inventory from one location where inventory counts have already been taken to another location where they have yet to be counted. Altering inventory counts may also result in double counting.

Earnings Per Share (EPS): It is the most commonly used ratio, and measures the profitability of an organization. When net income is overstated or cost profitability of an organization. When net income is overstated, earnings per share increases.

Gross profit (margin) ratio: It is calculated by dividing gross profit by sales.

Inventory turnover ratio: It is computed by dividing the cost of goods sold by the average inventory and is useful for determining whether inventory is overstated or the cost of goods sold is understated.

Overestimating inventory: It can occur by applying incorrect sampling methods. When inventory is estimated using sampling or projection techniques, the company can apply incorrect methods to overstated ending inventory.

Working capital turnover ratio: It is calculated by dividing net sales by average working capital (current assets - current liabilities) for a period.

## SelfAssessment

1. Why might a company want to understate net income?

A. To increase profits

B. To increase the stock price
C. To gain consumer confidence
D. To pay less taxes

2. Reported revenue and sales account balances that appear too high are examples of:
A. Analytical symptoms
B. Documentary symptoms
C. Lifestyle symptoms
D. Verbal symptoms

3. Horizontal analysis is a method that:
A. Examines financial statement numbers from period to period.
B. Examines percent changes in account balances from period to period.
C. Examines transactions from period to period.
D. Examines ratios from period to period.

4. Adding fictitious receivables will usually result in a(n):
A. Sales return percentage that remains constant.
B. Increased sales discount percentage.
C. Increase in accounts receivable turnover.
D. Increase in the number of days in receivables.

5. Unsupported revenue-related balances and missing documents in the revenue cycles are examples of:
A. Analytical symptoms
B. Documentary symptoms
C. Control symptoms
D. Perceptional symptoms

6. Accounts that can be manipulated in revenue fraud include all of the following except:
A. Accounts Receivable
B. Bad Debt Expense
C. Inventory
D. Sales Discounts

7. Which financial ratio is not useful in detecting revenue-related fraud?
A. Gross profit margin ratio
B. Account receivable turnover ratio
C. Asset turnover ratio
D. Debt Equity ratio

8. The asset turnover ratio measures:
A. The average time an asset is used by the company
B. The average useful life of capital assets
C. Sales that are generated with each dollar of the assets
D. Assets that are purchased with each dollar of sales

9. Which of the following is a possible scheme for manipulating revenue when returned goods are accepted from customers?

A. Understate allowance for doubtful accounts (thus overstating receivables)
B. Record bank transfers when cash is received from customers
C. Write off uncollectible receivables in a later period
D. Avoid recording of returned goods from customers

10. Comparing recorded amounts in the financial statements with the real-world assets they are supposed to represent would be most effective in detecting:

A. Cash and inventory fraud
B. Accounts payable fraud
C. Revenue-related frauds
D. Accounts receivable fraud

11. Lifestyle symptoms are most effective with:

A. Revenue-related financial statement frauds
B. Inventory-related financial statement frauds
C. Employee frauds
D. Accounts payable financial statement fraud

12. Which of the following is not an inventory-related documentary symptom?

A. Duplicate purchase orders
B. Missing inventory during inventory counts
C. Unsupported inventory sales transactions
D. Weaknesses in the inventory counting process

13. Which of the following ratios would not generally be used to look for inventory and cost of goods sold-related frauds?

A. Accounts payable turnover
B. Gross profit margin
C. Inventory turnover
D. Number of days' sales in inventory

14. _____ involve the seller holding goods for the buyer because the buyer may not be ready or able to accept shipment at the time of the order.

A. Cutoff problems
B. Overestimating inventory
C. Bill-and-hold sales
D. Consigned inventory

15. Which of the following is one of the fraud schemes for purchase inventory transactions?

A. Record purchases too late
B. Record returns in an earlier period
C. Do not record COGS
D. Overstate discounts

## Answers forSelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | D | 2. | A | 3. | B | 4. | D | 5. | B |
| 6. | C | 7. | D | 8. | C | 9. | D | 10. | A |
| 11. | C | 12. | D | 13. | A | 14. | C | 15. | A |

## Review Questions

1. What are some common revenue-related financial statement fraud schemes?
2. What are some possible ways to proactively search for revenue-related financial statement fraud schemes?
3. Examine the importance to follow up on revenue-related fraud symptoms?
4. Explain some of the most common inventory-related financial statement fraud schemes?
5. Explain the ways to proactively search for inventory financial statement fraud schemes?
6. What are common-size financial statements?
7. Why do you suspect that revenue-related financial statement fraud schemes are the most common and inventory-related fraud schemes are the next most common?
8. What is the effect on net income of not recording sales returns?
9. What is the effect on the net income of overstating ending inventory?
10. How can comparing statement amounts with actual assets help determine if fraud is present?

## Further Readings


- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. (2009). *Forensic Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.


### Web Links

- https://www.alphainvesco.com/blog/revenue-recognition-fraud/
- https://www.alphainvesco.com/blog/inventory-manipulation/
- https://www.fm-magazine.com/issues/2018/feb/prevent-inventory-fraud.html

# Unit 09: Consumer Fraud

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the meaning of Consumer fraud.
- explain the meaning and mechanism of Identity theft.
- summarize the ways of converting personal information to financial gain by fraudsters.
- summarize the ways of stealing a Victim's identity by fraudsters.
- summarize the preventive measures consumers should take to protect themselves from Identity theft.
- illustrate the various types of consumer scams.
- explain investment scam.
- summarize the various work-at-home schemes.
- illustrate telemarketing fraud.
- summarize red flags that signal potential consumer and investment scams.

## Introduction

According to Experian's 2022 Global Identity and Fraud Report, more than half of Indians surveyed feel most vulnerable to online fraud over the previous year, encountering fraud primarily on social media sites (38%), payment system providers (30%), and online gaming platforms (30%). A survey by Experian has found that almost one-third of Indian consumers have been victims of online fraud. More than half of the Indian consumers surveyed reported concern about fraud and identity theft and see a significant rise with today's growing fraud risk due to digitalization. The report also found that 7% of Indian consumers surveyed reported that at least one of the fraud incidents resulted in substantial monetary or reputational damage. This was the highest among the APAC regions. Meanwhile, 12% of Indian respondents' friends and family also suffered substantial monetary losses due to fraud incidents. The report found that Indian consumers are most vulnerable to fraud on Social Media Sites and apps followed by payment system providers and online gaming platforms. Indian consumers are highly vulnerable to suffering from online fraud on e-commerce marketplaces (29%), on online branded retailer sites (25%), and so on streaming service

platforms (25%). India has the highest rate of fraud in these categories out of the six APAC markets surveyed.

Neeraj Dhawan, Country Manager, Experian India says "There has been an exponential rise in digital payments in India, driven by the increased adoption of technology, making consumers and businesses susceptible to new and innovative types of online fraud. With the boom in digital payments, consumers and businesses need to remain vigilant and aware of emerging fraud trends and understand the risks involved in online transactions. Considering these facts, it has become relevant to study about consumer fraud, thus consumer fraud and its types are discussed in this unit.

## 9.1 Consumer Fraud and its Seriousness

Consumer fraud is a very serious problem in India and elsewhere in the world. With advances in technology, consumer fraud is on the increase. Consumer fraud is any fraud that targets individuals as victims. For example, consumer fraud can involve telephone fraud, magazine fraud, sweepstakes fraud, foreign money offers (such as Nigerian money scams), counterfeit drugs, Internet auctions, identity theft, and bogus multilevel marketing schemes.

Over 27 million Indian adults experienced identity theft in the past 12 months, says Norton report (2021)

A new cybersecurity report records responses from a total of 1,000 Indian adults and finds that around 60 per cent of them have been a victim of cybercrime within the last year. A report indicates that 59 per cent of Indian adults have been a victim of cybercrime in one way or another in the past 12 months. These victims have collectively spent 1.3 billion hours trying to resolve these issues. Even RBI acknowledged on December 8, 2021 that cyber security and digital frauds are the two major challenges in rolling out a central bank digital currency. In fact, at least 41% of citizen whose personal data was compromised allege that it was done by their telecom or banking service providers since majority of Indians have to share their personal financial details like a PAN card with multiple entities like banks, telos, loan or insurance agencies, digital payment apps, hotels and airlines, government offices, etc.

India has the third-highest number of users compromised after the US and Iran, as per report on country-wise data breach statistics from Netherlands-based Virtual Private Network (VPN) provider Surfshark.

Information was stolen from an 86.6 million user accounts in India through "9 big data breaches in 2021, including Domino's India and Air India cases. A hacker can sell your personal data in bulk to companies that will use it to target you with unsolicited commercial communications, including spam calls, SMS, emails, and WhatsApp messages.

## 9.2 Identity Theft

Identity theft is one of the pressing issues faced by all the countries in the world. No country is spared as identity theft has become a frequent happening in every nook and corner. In India, Identity theft has been found to be the rapidly growing white collar crime which has affected numerous individuals and it remains to be the leading type of data breach.

Identity theft is when a fraudster acquires personal, critical, and essential information of another individual, typically comprising personal and/or financial data, and then uses this information to indulge in any irregular activity, which is more often than not a fraud.

When someone makes unauthorized or fraudulent use of your personal or financial details, it is known as identity theft. It can pertain to your bank account, credit card, email ID, Aadhaar, PAN, or even your social medial account.

### Identity Theft: Legal consequences

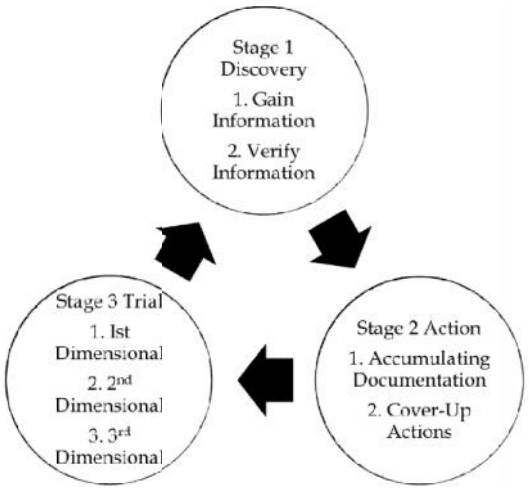
Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. - Sec. 66C of The Information Technology Act, 2000

### Identity Theft: Types

- Financial identity theft (using another's identity to obtain goods and services)
- Criminal identity theft (posing as another when apprehended for a crime)
- Identity cloning (using another's information to assume his or her identity in daily life)
- Business/Commercial identity theft (using another's business name to obtain credit)

### How Identity Theft Occurs

Perpetrators of identity theft follow a common pattern after they have stolen a victim's identity. To help you understand this process, we have created the "identity theft cycle." Although some fraudsters perpetrate their frauds in slightly different ways, most generally follow the stages in the cycle shown in the Figure given below:




### Stage 1. Discovery

1. Perpetrators gain information.

2. Perpetrators verify information.

### Stage 2. Action

1. Perpetrators accumulate documentation.

2. Perpetrators conceive cover-up or concealment actions.

### Stage 3. Trial

1. 1st dimensional actions-Small thefts to test the stolen information.

2. 2nd dimensional actions-Larger thefts, often involving personal interaction, without muchchance of getting caught.

3. 3rd dimensional actions-Largest thefts committed after perpetrators have confidence thattheir schemes are working.

### Stage 1: Discovery

The discovery stage involves two phases: information gathering and information verification. This is the first step in the identity theft cycle because all other actions the perpetrator takes depend upon the accuracy and effectiveness of the discovery stage. A powerful discovery stage constitutes a solid foundation for the perpetrator to commit identity theft. The smarter the perpetrator, the better the discovery foundation will be. If a perpetrator has a weak foundation, the evidence gathered will less likely to support a high-quality identity theft, which minimizes the victim's overall financial losses.

During the gaining information phase, fraudsters do all they can to gather a victim's information. Examples of discovery techniques include such information-gathering techniques as searching trash, searching someone's home or computer, stealing mail, phishing, breaking into cars or homes, scanning credit card information, or using any other means whereby a perpetrator gathers information about a victim.

During the information verification phase, a fraudster uses various means to verify the information already gathered. Examples include telephone scams, where perpetrators call the victim and act as a representative of a business to verify the information gathered (this is known as pretexting), and trash searches (when another means was used to gather the original information).

### Step 2: Action

The action stage is the second phase of the identity theft cycle. It involves two activities:accumulating documentation and devising cover-up or concealment actions.

Accumulating documentation refers to the process perpetrators use to obtain needed tools to defraud the victim.

Example

Using the information already obtained, perpetrators may apply for a bogus credit card, fake check, or driver's license in the victim's name.

Although the perpetrator has not actually stolen any funds from the perpetrator, he or she has now accumulated the necessary tools to do so. Any action taken by the perpetrator to acquire information or tools that will later be used to provide financial benefit using the victim's identity fall into this category.

Cover-up or concealment actions involve any steps that are taken to hide or cover the financial footprints that are left through the identity theft process.

Example, in this stage, a fraudster might change the physical address or e-mail of the victim so that credit card statements are sent by the financial institution to the perpetrator rather than the victim. These concealment actions allow the perpetrator to continue the identity theft for a longer period of time without being noticed.

### Stage 3: Trial

The trial stage involves those activities of the identity theft that provide perpetrators with financial benefits. There are three phases of the trial stage: 1st dimensional actions, 2nd dimensional actions, and 3rd dimensional actions. The trial stage is considered to be the most critical stage of the identity theft cycle because this is where the fraudster's work starts to pay off.

1st dimensional actions are the first frauds committed, mostly to test the effectiveness of fraud schemes and the stolen information.

2nd dimensional actions are the actions taken by a fraudster once initial trials have beensuccessful. These actions often involve face-to-face interactions with others.

3rd dimensional actions are thefts committed after the perpetrator has considerable confidence in the identity theft.

Once a fraudster has committed 3rd dimensional actions, he or she often discards the information of one victim and starts over with the discovery stage using another victim'sinformation. The following actual identity theft represents a 3rd dimensional theft:

I have been away from the United States for the past four years. Recently, I wanted to sell my house in California and contacted several real estate agents to discuss with them a listing for the house. I was informed by these realtors that my house has been rented to individuals whom I do not know. Someone is collecting the rent amounts on my house; furthermore, I have found upon checking with our county records that a certain individual has used my name, arranged to fake my signature, made a power of attorney in my name, received loans on my property, bought a business in my name, and accumulated a huge amount of financial burden with my name.

### How Fraudsters Convert Personal Information to Financial Gain

Once fraudsters have accessed personal information, they use that information to their financial benefit. Some of the common purchases made by identity theft perpetrators are as follows:

- Buying large-ticket items, such as computers or televisions.

- Taking out car, home, or other loans.
- Establishing phone or wireless service in victim's name.
- Using counterfeit checks or debit cards.
- Opening a new bank account.
- Filing for bankruptcy under the victim's name.
- Stealing a Victim's Identity.
- Reporting victim's name to police in lieu of their own.
- Opening new credit card accounts.
- Changing victim's mailing address.

### Stealing a Victim's Identity

Stealing a victim's identity isn't as difficult as it may seem. Fraudsters can obtain the information required to commit identity theft in numerous ways. Some of the more common types of information-gathering techniques used by identity thieves are as follows:

1. Posing as a legitimate official: Fraudsters gain personal information by posing as a legitimate employee, government official, or representative of an organization with which the victim conducts business.

2. Dumpster diving: Fraudsters rummage through consumers' trash- an activity sometimes called dumpster diving. Preapproved credit card applications, tax information, receipts containing credit card numbers, Social Security receipts, or financial records are valuable sources of information for identity thieves.

3. Skimming: Fraudsters skim victims' credit cards for information when they pay their bills. Skimming is a process where fraudsters will use an information storage device to gain access to valuable information when a credit card is processed.

- At Restaurants
- At ATM machines or gas stations
- By store clerks

Stealing a victim's identity isn't as difficult as it may seem. Fraudsters use numerous ways to get the information required to commit identity theft. Some of the more common types of information gathering techniques used by identity fraudsters are:

1. Fraudsters gather information from businesses.

They accomplish this by stealing information from their employer, hacking into organizations' computers, or bribing/conning an employee who has access to confidential records.

2. Fraudsters steal wallets or purses to gain confidential information or identification. Valuable information is contained in almost every wallet.

3. Fraudsters sneak into victims' homes and steal their information.

4. Fraudsters steal mail, which can include bank information, checks, credit card information, tax information, or preapproved credit cards.

5. Fraudsters complete a "change of address form" at the local post office and have victims' mail delivered to a PO box or another address of the fraudster's convenience.

6. Fraudsters engage in shoulder surfing where criminals will watch consumers from a nearby location as they give credit card or other valuable information over the phone.

7. Phishing: Phishing is a cybercrime in which a target or targets are contacted by email, pop-up messages, by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

8. Smishing: Smishing messages often appear to be from a legitimate source, such as a well-known company or government agency. It may even include urgent language or threats in an effort to get

victims to act quickly. In some cases, the message may also include a link that directs victims to a fake website where they are prompted to enter personal information or download malware.

"We have detected unusual activity on your account. Please call this number to speak to a customer service representative."

"You have won a free gift card! Click here to claim your prize."

9. Vishing: Vishing is almost identical to smishing, except cybercriminals use VoIP (Voice over IP) to place phone calls to trick victims instead of SMS (short message service) messages.

10. Spoofing: It is an identity theft where a person is trying to use the identity of a legitimate user. Phishing is where a person steals the sensitive information of user like bank account details. Spoofing can be phishing in part.

**How to minimize the Risk of Identity Theft?**

- Guard your mail from theft
- Safeguard all personal information
- Guard trash from theft
- Protect wallet and other valuables
- Opt out of preapproved credit cards
- Check your personal credit information (credit report) at least annually
- Guard Social Security card and numbers
- Protect passwords
- Don't save login credentials
- Protecting the home
- Protect the computer
- Never disclose your personal information or data
- Avoid unsafe ATMs
- Shred or discard physical identity documents appropriately

## 9.3 Other Types of Consumer and Investment Scams

Let's discuss various other types of scams that target consumers as their victims briefly.

- Foreign Advance-Fee Scams
- Work-at-Home Schemes
- Telemarketing fraud
- Scams That Prey on the Elderly

**Foreign Advance-Fee Scams**

Foreign advance-fee scams have been around for years; however, with the advent of the Internet, they have recently become much more widespread and common. Unfortunately, many individuals have become victim to this form of consumer fraud.

Foreign Advance-Fee Scams

- Nigerian Money Offers
- Other Foreign-Advance Fee Scams
- ✓ Clearinghouse scam
- ✓ Purchase of real estate scam
- ✓ Sale of crude oil at below market price
- ✓ Disbursement of money from wills

**Nigerian Money Offers**

Nigerian money offers are a form of foreign advance-fee scams where individuals from Nigeria or another (usually underdeveloped) country contact victims through e-mail, fax, or telephone and offer the victim millions of dollars. The catch is that in order to transfer the victim these monies, it is necessary to provide name and bank account numbers, including routing numbers, etc., so the money can be transferred.

### Nigerian Money Offers: Key Characteristics

The first characteristic is that it involves the promise of money.

The second characteristic of this fraudulent offer is that it asks for help.

Third, the perpetrator will try to build a relationship of confidence with the victim.

Fourth, nearly all fraudulent money offers ask that the victim respond immediately and confidentially.

Fifth, this offer makes the victim feel like he or she is the only person to receive this "special" opportunity. However, literally thousands of people are getting this exact same e-mail referring to such kind of offers daily.

Sixth, these kind of offer states that it is necessary to meet "for a face-to-face meeting outside Nigeria (country)." This request is again to instill confidence. Meetings such as these never take place, or, if they do, victims never know the true identity of the perpetrator or the reason for the meeting.

Seventh, nearly all fraudulent money offers will claim to have strong ties to high-ranking foreign officials.

Many fraudulent money offers will also send official-looking documents. These documents are always forgeries; yet, to many victims they add credibility to the perpetrators' claims. Often, fraudulent money offers will also ask victims to send their bank account number to show that the victim is willing to accept the offer. Other offers will ask victims to pay large "fees" to process the transaction. Once a victim responds to the e-mail, or has been deceived one time, the perpetrator will continue to have the victim pay transaction fees each time telling the victim that this is the last fee required.

### Other Foreign-Advance Fee Scams

A **clearinghouse scam** involves a victim receiving a letter that falsely claims the writer represents a foreign bank. This foreign bank is supposedly acting as a clearinghouse for venture capital in a certain country. The fraudulent company will try to get victims to invest in foreign venture capital companies for high returns. To give the impression that they are legitimate, the perpetrators will set up bank accounts in the United States.

When the victims transfer money into the domestic account, the perpetrators quickly transfer the money overseas where it will never be seen again. Some clearinghouse scams will actually give back a portion of the original investments in the form of dividends.

However, such transfers are made only to give the victim more confidence in the scam so that the victim will invest additional money. Eventually, the money is transferred and lost.

**Purchase of real estate**scam usually takes the form of someone trying to sell a piece of real estate or other property to the victim. Perpetrators will see advertisements for land (or other assets) being sold and send possible victims letters offering to purchase the property on behalf of a foreign concern. The victims are defrauded when they agree to pay "upfront fees" to a "special broker." Once paid, the victim will never hear from the perpetrator again.

**Sale of crude oil at below market price**is another type of foreign advance-fee scam. In this scam, the victim receives an offer to purchase crude oil at a price well below market price. However, in order to receive these "below market prices," it is necessary to pay special registration and licensing fees. Once the victim pays these fees, the seller disappears.

**Disbursement of money**from wills is a foreign advance-fee scam that is becoming ever more popular. In this scam, perpetrators con charities, universities, nonprofit organizations, and religious groups.

These organizations will receive a letter from a mysterious "benefactor" interested in contributing a large sum of money. However, to get the money, the charity is required to pay inheritance taxes or government fees. Once these taxes and fees are paid, the victims are unable to contact the benefactor.

### *Other Foreign-Advance Fee Scams: Key Characteristics*

They all come from an unknown party who claims to have access to large sums of money or assets.

The perpetrators are always willing to transfer that money or other assets to the victims, but only after money or information is extracted from the victims.

The perpetrators are not well-known, and there is usually some urgency to participate.

### Work-at-Home Schemes

The rising trend of working online from home has led to more opportunities to people, but it also posed new challenges to job aspirants as many find it hard to discern actual offers from fraudulent schemes. Online calls and data entry jobs are among the simplest remote work opportunities but these are also the favorites for scammers who trap unsuspecting victims and vanish after duping them of money.

- ✓ Unemployment and fraudulent schemers

The unemployment rate in India rose to 8.30 per cent in December 2022, the highest in 16 months, according to data from the Centre for Monitoring Indian Economy (CMIE).

As of January 13, 2023, the average unemployment rate in India is 7.85 per cent while it stands at 9.44 per cent in the urban areas, as per CMIE. The schemers trap desperate and innocent job-seekers with lucrative monthly salaries. They ask aspirants to make a security deposit to cover the cost of the services provided and then dupe them of their money before the start of their work or within a month or two of joining. The victims are duped of their money either before the assignment starts or after a month or two of working.

Multiple police investigations have revealed that fraudsters are not restricted to India, as per media reports. There have been reports of people falling prey to scams from people based in the Middle East. Often, the 'employers' or 'recruiters' are well-spoken professionals with fake websites and profiles that seem legitimate to a common person, thus adding credibility to their traps.

You can find people marketing fraudulent work-at-home schemes on the telephone, in chat rooms, on the Internet, through telephone polls, as banners or advertisements on automobiles, through the use of fliers, on message boards, in classified ads, and through all other types of communications media.

### Work-at-Home Schemes: Common Scams

There are many different scams that potential remote workers must sift through. Most work-from-home scams fall into two categories:

1. Potential employees work from home as part of a supposed company that often does menial work like envelope stuffing or assembly. These scams are often built on roping other people into the scam, too.

2. Potential workers start their own business with the help of the scam, only after they buy into or pay money to get “certified” or get the “starter kit.”

While most scams fall into these two categories, individual job listings can mix up the details enough and provide enough convincing information to make them seem like legitimate careers.

- ✓ Medical Billing
- ✓ Envelop or Mail Stuffing
- ✓ Chain Letter Scams
- ✓ Product testing
- ✓ Craft Assembly
- ✓ Starting an internet Business

- ✓ Pay for Training
- ✓ Mystery Shopping
- ✓ MLM Marketing

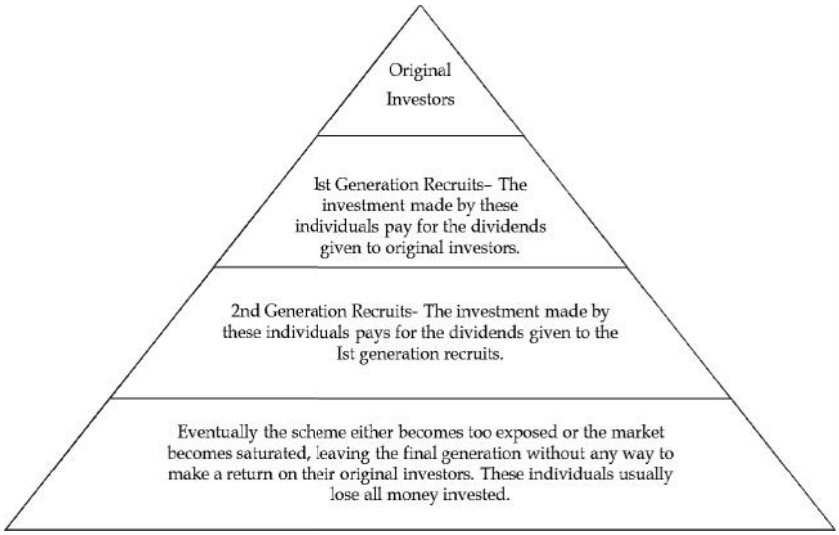
### Multilevel Marketing

Just about everyone has been approached at some time or another to join a multilevel marketing (MLM) company. When structured correctly, with honest people, multilevel marketing is a legitimate form of business.

In fact, it is really another marketing approach from which organizations may choose. In most multilevel marketing programs, company representatives act as sellers of real products such as facial creams, health aids, detergents, and foot supplements. These individuals are independent distributors of a legitimate business.

Some multilevel marketing jobs are legitimate, so this one might be the toughest to differentiate real from fake. The best distinction between the two is that in real MLM businesses, the workers make commission on the sales of their product. It's important to ask how much money the majority of the entry-level salespersons make, and not to get wrapped up in the amount the high-level people make.

"The Federal Trade Commission notes this important point, If anyone suggests recruiting is the real way to make money, know this: MLMs that survive on recruiting new participants rather than retail sales are pyramid schemes. Pyramid schemes are illegal, and the vast majority of participants lose money." The Structure of a Pyramid Scheme is given in following Figure.




### Work-at-Home Schemes: Red Flags

Much like other get-rich-quick schemes, anything that seems too good to be true probably is and should be avoided. "Do your research and trust your gut," says Eleni Cotsis, a specialist in remote work and the founder of Women Entrepreneurs of Medellin. "If it feels like a pyramid scheme or a scam, it probably is."

In addition to a gut-feeling, there are clear-cut signs that a work-from-home opportunity isn't on the up-and-up. Job-seekers should keep a particularly close look-out for these common signs:

- ✓ They ask for money up-front
- ✓ You don't speak with or see a real person
- ✓ They use a generic email account (Gmail, AOL, Yahoo, etc.)
- ✓ The job description lacks detail or is mostly "fluff".

### Telemarketing Fraud

"Really it's the truth," replied the confident voice on the other end of the telephone. "Normally,I don't make these kinds of calls. I've got a whole staff to do that. I have 15 years of experience in the

business. I'm currently in charge of a large staff. I have over 600 clients and manage over $60 million for those clients. I don't even need this account-but I want it-this is a great opportunity for you."

The script above is typical of the kind of messages used throughout the United States by telemarketing fraud artists. Fraudsters set up giant rooms (referred to as boiler rooms) in rented offices where they train salespeople to find and defraud victims. These professional fraudsters move from city to city using different names. Calling people in other cities and statesis an effort to hinder law enforcement, these con artists swindle victims out of money. Gatheringcompiled lists from magazine subscriptions, they identify investors believed to be good targets.New recruits are given scripts like the one above and receive specialized training to counterevery possible objection. These recruits hook victims through promises of no-risk investments,secrets tips, and incredible rates of returns.

The North American Securities Administrators Association, an association of state investment regulators, estimates that unwary investors lose about $1 million every hour to investment fraud promoted over the telephone. Throughout the last two decades, the telephone has become a major tool used to defraud innocent victims. The opportunity to speak with a person directly makes telemarketing fraud more effective than Internet or mail-based approaches. Furthermore, the lack of face-to-face contact gives fraudsters added schemes and opportunities to commit fraud. Offenders can act as corporate or government employees without the victims' knowledge. Younger perpetrators can impersonate middle-aged authority figures to add credibility with older victims. Fraudsters can call anywhere anytime, making it possible to focus on more likely victims.

In August 2004, when Hurricane Charley swept through Florida and destroyed countless homes, thousands of people applied for government grants to help cover the cost of damage. Fraudsters used this opportunity to their advantage and committed fraud in two ways: First, fraudsters began calling Florida hurricane victims and telling them that to process their government grants, they would need their bank account numbers and other personal information. As if the victims of the hurricane had not been through enough, they quickly saw their bank accounts drained. Second, fraudsters would call hurricane victims and tell them that in order to process their government grant they needed to pay up-front fees. Fraudsters had the victimssend these fees to PO boxes, where the fraudsters quietly took the money and vanished. Hurricane Charley is just one example of how fraud perpetrators use disasters and any other event they can to identify susceptible victims and perpetrate fraud.

### Scams That Prey on the Elderly

As with all consumer frauds, those who are most susceptible are usually the uneducated and theelderly. However, the elderly are more susceptible to telemarketing fraud than almost any other type of fraud. Fraudsters target the elderly for several reasons:

First, many older individuals are extremely lonely and fraudsters use this loneliness to build a relationship of trust.

Second, when elderly people are conned out of money, they rarely tell family and friends or even report the incident. The elderly are usually extremely embarrassed that they have been a victim of fraud. They are also afraid if they report the fraud, family members may deem them unable to take care of themselves and take away their financial responsibility and independence.

Third, the elderly persons are extremely trusting and many do not believe that someone would actually take advantage of them. Once defrauded, these gullible victims often go into a state of denial.

Fourth, because fraudsters are able to build such strong ties between themselves and the victim, fraudsters will con elderly victims out of money seven or even eight times before the victim refuses to pay more money. Remember, these fraudsters are masters of manipulation. They focus on manipulating human traits such as greed, fear, excitement, and gullibility.

Because the elderly people are susceptible and reluctant to report fraud, it is important that family and friends of the elderly exercise special caution.

Many parent-child relationships have been strained and even irreparably damaged because children have approached the issue in a confrontational and/or threatening manner. Fraudsters will even manipulate a victim's emotions to believe that they are more concerned about the victim's

welfare than the victim's own family is, convincing the victim that his or her family is greedy and wants his or her money.

As with all fraud, the most effective way to combat telemarketing fraud is through prevention. Education is the best form of prevention. Therefore, it is a good idea to educate parents, grandparents, or anyone else you believe might be susceptible to telemarketing fraud. Remember, because fraudsters need the voluntary participation of the victim, possible victims can defend against the fraud artist by just saying "no" or hanging up the telephone.

### Safeguards Against Telemarketing Fraud

There is never a legitimate reason to give Social Security, credit card, or other information overthe telephone unless you initiate the call. If anyone ever asks for Social Security numbers or personal information, it should send a red flag that something isn't right. Fraudsters sometimes even act as government officials or other representatives to get this vital information. It is always risky to provide credit or bank account information over the telephone whenmaking purchases. Consumers should only provide this information when they are actuallypurchasing something and have initiated the transaction. Even if the company is completelylegitimate, the salesperson or representative who enters a consumer's information may capturethe victim's credit card number, expiration date, and verification number and use the information later to commit fraud.

Language such as, "this special offer will no longer be available after today, "or "there are only a few products left-hurry and buy now" are also signals of a fraudulent transaction.

Magazine sweepstakes and prize-winning scams are often perpetrated via the telephone. Fraudulent companies usually require individuals to buy something or pay a fee to claim a prize. However, it is illegal for a company to require consumers to buy something or pay a fee to claim a prize. Therefore, if a proposal or contest requires up-front cost, it is probably fraudulent.

Remember, telemarketers will use any language they can to deceive possible victims. They are professionals and make money through manipulating victims' emotions. Consumers should never believe any promise of easy money. If someone promises money with little or no work, loans or credit cards with bad credit, or any type of money-making investments with no risk, it should signal that something is not right.

When entering into transactions over the telephone, it is critical that individuals know who they are dealing with. If someone claims to be from a certain company or organization, consumers should verify that claim by calling a legitimate phone number of the organization they are dealing with before giving out any personal information.

Avoid Sales Calls

- To minimize their risk to telemarketing fraud, consumers can avoid getting on marketing or calling lists by choosing to register with the national "do not call" registry.
- In India, Telecom Regulatory Authority of India (TRAI) has created a NDNC Filter i.e. National Do Not Call Registry which is fully run by Indian Govt. The main purpose for creation of NDNC is to prevent unwanted Marketing SMS and calls from Telemarketers.
- If you do not want to receive any promotional SMS or calls from any company, you can add your number in NDNC registry.

### Investment Scams

Investment fraud is any fraud that is related to stocks, bonds, commodities, limited partnerships, real estate, or other types of investments. In investment fraud, perpetrators usually make fraudulent promises or misstatements of fact to induce people to make investments. Investment frauds are often set up as Ponzi schemes. Investments frauds can occur within or outside business organizations. An example of investment fraud in a business was the loans made by General Motors Acceptance Corporation (GMAC) to a Long Island, New York, automobile dealer.

John McNamara, a wealthy car dealer, conned $436 million from GMAC. He first set up a company, Kay Industries, to produce invoices showing he was buying vans. The vans didn't exist. Then he sent inventories to GMAC to get a 30-day loan, worth about $25,000, for each van. Over seven years, he got $6.3 billion in loans, and he used most of the money to pay off old loans. He paid back

a total of $5.8 billion over the seven years. He pocketed $436 million-about 7 percent of the total loans-and invested it in real estate, gold mines, oil businesses, and commodities brokerages.

While GMAC thought it was loaning money to a legitimate car dealer, it was really investing in a classic Ponzi scheme (a scheme in which early investments are repaid with subsequent investments; see previous discussion). The only difference between this investment scam and one that is perpetrated outside an organization was that this investment scheme had only one investor, GMAC.

### Investment Scams: Red Flags

There are numerous red flags or fraud symptoms that signal potential investment fraud. Anyone considering investing money or other assets in any organization, real or fictitious, should watch for the following symptoms, which have been associated with numerous investment scams:

- Unreasonable promised rates of return
- Investments that do not make sound business sense
- Pressure to get in early on the investment
- Use of a special tax loophole or a tax avoidance scheme
- Unaudited financial reports or adverse opinions given on financial reports
- Investments that assume continued inflation or appreciation in predicting attractive ratesof return that are unrealistic over time
- Investment success that is dependent on someone's "unique expertise" (such as an uncanny ability to predict commodity prices or unusually good salesmanship) for financial success
- Representation of the emotional desirability of holding an investment as its principalattraction
- Insufficientverification or guarantee of an investment Dependency on high financial leverage for success
- Investor liability for debts that are not paid
- Luxurious lifestyles of principals, even though the business is relatively new
- An investment that isnot suitable for your risk tolerance
- Pressure to put all your savings into a particular investment
- Inability to pull out or liquidate the investment
- Inducements that make investors feel sorry for the principals and/or put in additionalmoney to help them overcome temporary problems.

## Summary

There has been an exponential rise in digital payments in India, driven by the increased adoption of technology, making consumers and businesses susceptible to new and innovative types of online fraud.

With the boom in digital payments, consumers and businesses need to remain vigilant and aware of emerging fraud trends and understand the risks involved in online transactions.

SEBI alerted its users about Phishing links and issue a press release listing some following preventive measures:

- Never provide personal information, such as account numbers, passwords, or any combination of sensitive information that could be used fraudulently, over text message, phone, or e-mail.
- Always keep in mind that passwords, PINs, TINs, and other personal information are completely confidential and are not shared with anyone outside of the Bank's employees or service staff.
- Only enter your user id and password on the authenticated page.

- Please ensure that the URL of the login page begins with the text 'https://' and not 'http://' before entering your user id and password.
- Only provide your personal information if you initiated the call or session and the counterpart has been duly authenticated by you.

To minimize their risk to telemarketing fraud, consumers can avoid getting on marketing calls.

In India, Telecom Regulatory Authority of India (TRAI) has created a NDNC Filter i.e. National Do Not Call Registry which is fully run by Indian Govt. The main purpose for creation of NDNC is to prevent unwanted Marketing SMS and calls from Telemarketers.

If you do not want to receive any promotional sms or calls from any company, you can add your number in NDNC registry.

## Keywords

Craft assembly: It is a scam where perpetrators promise high pay for working on different projects. These projects can include anything from wooden calendars, to paper towel holders, to hair clips, and even holiday decorations. Victims are usually required to purchase costly materials, equipment, and training.

Identity Theft: Identity theft as a term refers to Fraud that involves stealing money or getting other benefits by pretending to be someone else. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions.

Mail stuffing: It is a scam where consumers respond to an advertisement that promises income simply for stuffing envelopes.

Phishing: It is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

Skimming: It is a hi-tech method by which thieves capture personal or account information from a credit card, driver's license, or even a passport. An electronic device used to capture this information is called a "skimmer".

Smishing: It is a type of phishing scam where attackers send SMS messages (or text messages) to trick victims into sharing personal information or installing malware on their devices.

## SelfAssessment

1. The major reason that elderly people are so susceptible to telemarketing fraud is that they:

A. Are often financially in need.
B. Have an excess amount of cash to invest.
C. Are often lonely and enjoy talking to friendly callers.
D. Are none of the above.

2. Consumers should provide credit card numbers or bank account information over the telephone only when:

A. They initiated the call and are purchasing a legitimate product.
B. They are asked to give the information.
C. The entity receiving this information is a legitimate company.
D. They feel confident that the receiving entity will protect such information.

3. What is the best defense against consumer fraud?

A. Add your number in NDNC registry
B. Purchasing credit card insurance

C. Educating yourself about credit card risks
D. Calling the Ministry of Commerce and Industry

4. What does "https" stand for?
A. Hypertext transfer point secure
B. Hypertext transfer protocol system
C. Hypertext transfer protocol sign
D. Hypertext transfer protocol secure

5. Which of the following is not listed as a common characteristic of Nigerian scam letters?
A. The promise of money to lure victims
B. Urgency to invest quickly
C. Picture of the perpetrator to assure victims
D. Strong ties to high-ranking foreign officials to lure victims

6. What is one way to determine if a Web site is secure or not?
A. Look for the official logo of the company you want to deal with
B. Look for an "s" after the "http" in the URL of the Web site
C. Click on a link to see if it works
D. Call the FTC and ask about the ISP address of the Web site

7. Those most susceptible to consumer fraud are often:
A. Uneducated and elderly
B. Wealthy and prominent
C. Troubled with credit card debt
D. Lonely and depressed

8. NDNC stands for:
A. New Do Not Call Registry
B. National Do Not Communicate Registry
C. National Do Not Call Registry
D. National Depository for Non-Call

9. MLMs that survive on recruiting new participants rather than retail sales are:
A. Legitimate Schemes
B. Ponzi Schemes
C. Pyramid Schemes
D. Bogus Mystery Investment Schemes

10. The perpetrators will almost always refuse to pay the investor for the work rendered, declaring that the work does "not meet standards" in the following consumer fraud scheme:
A. Envelop or Mail Stuffing
B. Chain Letter Scams
C. Product testing
D. Craft Assembly

11. Using another's identity to obtain goods and services is an example of:

A. Financial identity theft
B. Criminal identity theft
C. Identity cloning
D. Business/Commercial identity theft

12. Using another's information to assume his or her identity in daily life is an example of:

A. Financial identity theft
B. Criminal identity theft
C. Identity cloning
D. Business/Commercial identity theft

13. _____ is a hi-tech method by which thieves capture personal or account information from a credit card, driver's license, or even a passport.

A. Posing as a legitimate official
B. Dumpster diving
C. Skimming
D. Vishing

14. _____ is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

A. Dumpster diving
B. Skimming
C. Vishing
D. Phishing

15. _____ is a type of phishing scam where attackers send SMS messages (or text messages) to trick victims into sharing personal information or installing malware on their devices.

A. Smishing
B. Vishing
C. Phishing
D. Spoofing

## Answers for SelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | C | 2. | A | 3. | A | 4. | D | 5. | C |
| 6. | B | 7. | A | 8. | C | 9. | C | 10. | D |
| 11. | A | 12. | C | 13. | C | 14. | D | 15. | A |

## Review Questions

1. Is it important to study consumer fraud? Justify
2. Illustrate identity theft?

3. What are some methods perpetrators use to steal a person's identity?
4. What are some proactive steps that consumers can take to minimize their risk of identity theft?
5. What are some examples of foreign advance-fee scams?
6. Explain the Nigerian money offer?
7. Compare a fraudulent multilevel marketing organization and a legitimate multilevel marketing organization?
8. How does consumer fraud affect the economies of entire countries?
9. Explain work-at-home related scam schemes.
10. Discuss other types of consumer fraud.
11. Explain the reasons behind the high chances of getting scam victims of elderly persons.

## Further Readings


- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., &Zimbelman, M. (2009). *Forensic Accounting and Fraud Examination* (Indian Edition ed.). Cengage Learning India Private Limited.


### Web Links

- https://cio.economictimes.indiatimes.com/news/digital-security/a-huge-chunk-of-indian-consumers-are-victims-of-fraud-experian/96198217#:~:text=Indian%20consumers%20are%20highly%20vulnerable,the%20six%20APAC%20markets%20surveyed.
- https://www.indiatoday.in/technology/news/story/over-27-million-indian-adults-experienced-identity-theft-in-the-past-12-months-says-norton-report-1792553-2021-04-19
- https://timesofindia.indiatimes.com/business/india-business/explained-what-is-identity-theft-and-how-you-can-protect-your-personal-data-online/articleshow/89968866.cms
- https://www.legalserviceindia.com/legal/article-1780-identity-theft-a-threat-to-society.html
- https://www.outlookindia.com/national/robbed-of-money-hope-and-hard-work-online-job-scams-is-trapping-the-indian-youth-amidst-job-dearth-news-253665

Dr. Razia Sehdev, Lovely Professional University

# Unit 10: Regulatory Measures for Curbing Corporate Fraud - 1

**CONTENTS**

## Objectives

After studying this unit, you will be able to:

- summarize the major legislations for regulating fraud in India.
- examine relevant provisions of the Companies Act, 2013 to curb or prevent corporate fraud.
- summarize relevant provisions of the Companies Act, 2013 to curb or prevent corporate fraud.
- summarize the relevant sections and their provisions dealing with curbing or preventing corporate frauds under the SEBI Act, 1992.

## Introduction

The legal environment plays a crucial role in determining the nature of corporate governance. The two important aspects of corporate fraud are: (1) de jure protection the protection offered under the laws and (2) de facto protection-the extent to which the laws have been enforced.

As provided in the Preamble to the Constitution of India, the Government must secure all its citizen's social, economic, or political justice. The Directive Principles of State Policy are fundamental in the governance of the country and they enjoin upon the State to apply these to direct its policy to sub-serve the common good and to see to it that the operation of the economic system does result in the concentration of wealth and means of production to the common detriment (Article 390b) and (c)). This unit analyses the major legislative provisions in India, governing corporate fraud specifically the Companies Act, 2013, and the Securities and Exchange Board of India Act, 1992.

## 10.1 Regulation of Corporate Fraud in India

The significant legislations for regulating corporate fraud in India are summarized in the following table:

| S. No | Name of the Act | Relevant Sections | Enforcement Authority | Appeal Against Order of the Authority/ Court |
|---|---|---|---|---|
| 1 | The Companies Act, 2013 | Sections 7(5), 7(6), 8(11), 34, 36, 38(1),46(5), 56(7), 66(10), 75(1), 132, 139, 140(5), 206, 207, 208, 209, 210, 211, 212, 213, 216, 217, 219, 220, 221, 222, 223, 224, 229, 241, 244, 251(1), 266(1), 339(3), 447, and 448 | National Company Law Tribunal<br>Relevant department under the Ministry of Corporate Affairs<br>Regional Director<br>Registrar of Companies<br>Central Government | National Company Law Appellant Tribunal<br>High courts |
| 2 | The Securities and Exchange Board of India Act, 1992, read with the SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities | Section 11, 11C, 11D, 12, 12A, 15A, 15B, 15C, 15D, 15E, 15F, 15G, 15H, 15HA, 15HB, 15K, 15L, 15R, 15T, 15V, 15Y, 15Z, 20, 23, 24, 24A and 27.<br>Regulation- | The Securities and Exchange Board of India | Securities Appellate Tribunal followed by Supreme Court |

| | | | | |
|---|---|---|---|---|
| | Market) Regulations,2003 | 2(1)(c) | | |
| 3 | The Benami Transactions (Prohibition) Act, 1988 | Sections 3, 4, 5, 6, 7, 8 | Civil Courts | High Courts<br>Supreme Courts |
| 4 | The Money Laundering Act, 2002 | Sections 4, 12, 13, 14, 66 | Adjudicating Authority | Appellate Tribunal, followed by High Court, and finally by the Supreme Court |
| 5 | The Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974 | Sections 3, 4, 5, 5A, 7, 8, 9, 10, 11, 12 and 12A | Central Government | High Courts |
| 6 | The Indian Penal Code, 1860 | Sections 11, 23, 25, 33, 53, 120A, 264, 403, 405, 408, 409, 410, 415, 416, 417, 418, 419, 420, 421, 463, 464, 465, 468, 470, 471, 477, 477A, 481, 482, 486, 487, 489 and 511 | District and Sessions Court | High Courts |

Source: Gupta, D. S. (2016). Corporate Frauds & their Regulation in India (First ed.). Bharat Law House PVT. LTD.

## 10.2 Relevant Provisions of the Companies Act, 2013

Although corporate frauds have been rampant in India and their detection and prevention are of prime concern for the government and the stakeholders. These frauds adversely affect the public at large, investors, customers, and employees. Earlier, there had been no effective measure to regulate such frauds in the country. The new legislation on companies has sought to bridge this gap in regulatory measures.

Various sections have been incorporated under the Companies Act, 2013, whereby fraud, being the major section to deal with fraud, has been adopted first time in the Companies Act, 2013. The major sections and the sections inter-related to the relevant sections focusing on curbing and preventing corporate are divided into three main categories as given below:

1) Offenses Punishable for Fraud

2) Oppression and Management

3) Inspection and Investigation of Books of Accounts by Registrar of Companies/Central Government/SEBI/SFIO

## 10.3 Offenses Punishable for Fraud

Fraud has to be controlled and it should be prevented only at an initial stage. The measures for the prevention and control of frauds can be divided into two categories:

(i) Pre-fraud Stage, i.e., action against persons likely to commit a fraud; and

(ii) Post-fraud Stage, Le, action taken, after committing fraud or to penalize the fraudster to deter other fraudsters.

For the first time, the Companies Act, 2013 has introduced provisions relating to 'fraud in section 447, and the penal provisions have been made in this section for offenses under different sections of the Act.

The various provisions dealing with offenses punishable for fraud are summarized below:

**Pre-fraud Stage**

**1. Fraud in respect of the Incorporation of a Company:**

A Company as an artificial person and on its incorporation, it becomes a legal person having a separate identity from its members. A company is not a citizen under the Constitution of India and does not enjoy fundamental rights guaranteed by Article 19 of the Constitution of India. Once the company is registered, it can be wound up only by Court. Sections 7(5), 7(6), and 8(11) of the Companies Act, 2013 deal with the action specified under Section 447.

***Section 447: Punishment for fraud***

Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, involving an amount of at least ten lakh rupees or one percent of the turnover of the company, whichever is lower shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud; Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.

Provided further that where the fraud involves an amount less than ten lakh rupees or one percent of the turnover of the company, whichever is lower, and does not involve public interest, any person guilty of such fraud shall be punishable with imprisonment for a term which may extend to five years or with a fine which may extend to fifty lakh rupees or with both.

Furnishing of false information with ROC concerning registration

***Section 7(5):***If any person furnishes any false or incorrect particulars of any information or suppresses any material information, of which he is aware in any of the documents filed with the Registrar in relation to the registration of a company, he shall be liable for action under section 447.

Persons liable for furnishing false information after incorporation of a company

***Section 7(6):***Without prejudice to the provisions of sub-section (5) where, at any time after the incorporation of a company, it is proved that the company has been got incorporated by furnishing any false or incorrect information or representation or by suppressing any material fact or information in any of the documents or declaration filed or made for incorporating such company, or by any fraudulent action, the promoters, the persons named as the first directors of the company and the persons making the declaration under clause (b) of subsection (1) shall each be liable for action under section 447.

Directors and even officers are liable if the company incorporated under Section 8 does not comply with the provisions applicable to section 8 company

***Section 8(11):***If a company makes any default in complying with any of the requirements laid down in this section, the company shall, without prejudice to any other action under the provisions of this section, be punishable with a fine which shall not be less than ten lakh rupees but which may extend to one crore rupees and the directors and every officer of the company who is in default shall be punishable with fine which shall not be less than twenty-five thousand rupees but which may extend to twenty-five lakh rupees.

Provided that when it is proved that the affairs of the company were conducted fraudulently, every officer in default shall be liable for action under section 447.

Example

(i) A company entered into a contract but did not disclose to the Registrar of Companies about the said contract at the time of incorporation of a company.

### (2) Frauds related to the Share Capital of a Company

Numerous sections under the Companies Act, 2013 deal with the raising of share capital and its treatment by a company, and offenses under those sections are liable to action under Section 447. These provisions are briefly described below: -

***(i) Raising capital by misstatement in the prospectus.***The penalty has been broadened in the new Companies Act and as per section 34, a person who has authorized to issue a prospectus containing an untrue and misleading statement shall be punishable under Section 447.

### Liability of persons for inclusion of untrue/misleading information in a prospectus

***Section 34:***Where a prospectus sued, circulated, or distributed under this Chapter, includes any statement which is untrue or misleading in form or context in which it is included or where any inclusion or omission of any matter is likely to mislead, every person who authorizes the issue of such prospectus shall be liable under Section 447:

### Immunity if the statement is immaterial and it was true at the time of issue of the prospectus

Provision: Provided that nothing in this section shall apply to a person if he proves that such statement or omission was immaterial or that he had reasonable grounds to believe, and did up to the time of issue of the prospectus believe, that the statement was true or the inclusion or omission was necessary.

Example

In Prospectus, the company stated that the company declared dividend for many years, but the dividend was paid out of capital profits realization and not out of trading income or profits. The prospectus containing this information is false and misleading information. (Rex. v Kyslant (1932) 1 K.B. 422)

***(ii) Fraudulently inducing others to invest money:***Any person who induces others to invest money by making statements that are false, deceptive, misleading, or deliberately concealing any facts, shall be liable for punishment for fraud under Section 447.

This offense is non-compoundable and investment means investing in all types of securities and not only limited to shares/debentures. Section 36 also provides punishment for inducing another person on false grounds to agree to obtain credit facilities from any bank or financial institution.

### Making any misleading statement/false promise to induce any person to agree with the company

***Section 36:***Any person who, either knowingly or recklessly makes any statement, promise or forecast which is false, deceptive or misleading, or deliberately conceals any material facts, to induce another person to enter into, or to offer to enter into, -

(a) any agreement for, or with a view to, acquiring, disposing of, subscribing for, or underwriting securities; or

(b) any agreement, the purpose or the pretended purpose of which is to secure a profit to any of the parties from the yield of securities or by reference to fluctuations in the vile of securities; or

(c) any agreement for, or with a view to obtaining credit facilities from any bank or financial institution, shall be liable for action under Section 447.

Example:

Submission to Bank/Financial Institution about a proposed agreement of takeover of a firm or company which has no relevance to the future business of the company.

***(iii) Personation for the acquisition of securities:***A person who makes an application in a fictitious name, make multiple applications in different names or in different combination of names for acquiring or subscribing for securities, or induces a company to allot or register any transfer of securities in a fictitious name, shall be liable for punishment under Section 447.

Applying share applications in a combination of names if a person's name is Raj Purohit Gupta, then an application can be made as:

(1) Raj Purohit Gupta

(ii) Purohit Raj Gupta

(iii) R.P. Gupta

(iv) Raj P. Gupta

(v) Gupta Raj P

(vi) Gupta Raj Purohit

***(iv) Issuance of Duplicate Share Certificates:***If a company issues duplicate share certificates to defraud, every officer of the company who is in default shall be liable for action under Section 447 of the Act.

Issuance of duplicate share certificates to defraud

Section 46(5):

If a company with the intent to defraud issues a duplicate certificate of shares, the company shall be punishable with a fine which shall not be less than five times the face value of the shares involved in the issue of the duplicate certificate but which may extend to ten times the face value of such shares or rupees ten crores whichever is higher and every officer of the company who is in default shall be liable for action under section 447.

(***v) Transfer or Transmission of Shares by Depository:***Where any depository or depository participant to defraud a person, transfers shares then, such depository or depository participant, besides the liability under the Depositories Act, 1996, shall be liable for punishment under Section 447 of the Act. In case of forged or fraudulent transfer of shares, the limitation period is not applicable to get justice from the Court/Competent Authority.

Depository liable in case of transfer of shares to defraud another

Section 56(7):

Without prejudice to any liability under the Depositories Act, 1996, where any depository or depository participant, intending to defraud a person, has transferred shares, it shall be liable under Section 447.

Example

The depositor or the company transfers the shares with the intent to decrease the shareholding of a particular group of a company.

(***vi) Reduction of Share Capital:***An officer of the company shall be liable for action under Section 447 of the Act if he knowingly conceals the name o any creditor who was entitled to object to the reduction of share capital or knowingly misrepresents the nature or debt amount or claim of any creditor or encourages or assists or concerned to any such concealment. The Court or competent authority gives due regard to the interest of creditors who may comment or object to the reduction of the share capital of a company.

### Liability of officer who knowingly conceals the particulars of a creditor

Section 66(10): If any officer of the company--

(a) knowingly conceals the name of any creditor entitled to object to the reduction;

(b) knowingly misrepresents the nature or amount of the debt or claim of any creditor; or

(c) abets or is privy to any such concealment or misrepresentation as aforesaid,

he shall be liable under section 447.

Example

Submission of application with Court or competent authority with a list of creditors and No Objection Certificate from those creditors only who have given their consent for reduction of capital while concealing the information about those creditors who objected to the reduction.

## 10.4 Post-Fraud Stage

### (1) Repayment of Deposits (Damages for Fraud): Sec. 75(1)

Section 75 of the new Companies Act provides that every officer of the company who is responsible for acceptance of any deposit shall be liable to action under Section 447, if such company fails to repay the deposits or any part thereof or any interest thereon, within the time specified, and if it is proved that the deposit was accepted with an intent to defraud the depositors or for any fraudulent purpose.

Acceptance of deposits more than the amount up to which companies are entitled to accept deposits.

### (2) Penalties on Auditors and their Firm: Sec. 132

The Central Government may, by notification, constitute a National Financial Reporting Authority (NFRA) to provide for matters relating to accounting and auditing standards under this Act.

**Did you know?**

What is NFRA?

National Financial Reporting Authority (NFRA) is being set up under the Companies Act, 2013 to take actions and penalize those members of Institute of Chartered Accountants of India, who are associated with ensuring compliance with accounting standards and policies It can also take action against the firm of Chartered Accountants.

### Objectives of NFRA

(a) make recommendations to the Central Government on the formulation and laying down of accounting and auditing policies and standards for adoption by companies or class of companies or their auditors, as the case may be;

(b) monitor and enforce compliance with accounting standards and auditing standards in such manner as may be prescribed.

(c) oversee the quality of service of the professions associated with compliance with such standards and suggest measures required for improvement in quality of service and such other related matters as may be prescribed, and

(d) perform such other functions relating to clauses (a), (b), and (c) as may be prescribed.

### Powers of NFRA

Notwithstanding anything contained in any other law for the time being in force, the National Financial Reporting Authority shall-

### Powers to investigate suo moto or on the reference of the Central Government

(a) have the power to investigate, either suo moto de on a reference made to it by the Central Government, for such class of bodies corporate or persons, in such manner as may be prescribed into the matters of professional or other misconduct committed by any member or firm of chartered accountants, registered under the Chartered Accountants Act, 1949:

**Powers of Civil Court**

(b) have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, respect of the following matters, namely:

(i) discovery and production of books of account and other documents, at such place and at such time as may be specified by the National Financial Reporting Authority;

(ii) summoning and enforcing the attendance of persons and examining them on oath;

(iii) inspection of any books, registers, and other documents of any person referred to in clause (b) at any place;

(iv) issuing commissions for the examination of witnesses of documents;

### Powers to impose a penalty on a professional after proof of misconduct

(c) where professional or other misconduct is proved, have the power to make an order for

(A) imposing penalty of-

(1) not less than one lakh rupees, but which may extend to five times of the fees received, in case of individuals; and

(II) not less than ten lakh rupees but which may extend to ten times of the fees received, in the case of firms;

(B) debarring the member or the firm from engaging himself or itself from practice as a member of the Institute of Chartered Accountant of India referred in clause (e) of sub-section (7) of section 2 of the Chartered Accountants Act, 1949 for a minimum period of six months or for such higher period not exceeding ten years as may be decided by the National Financial Reporting Authority.

### (3) Rotation of Auditors or Firm of Auditors: Sec. 139

The Companies Act, 2013 has a provision for the rotation of auditors or auditor's firm after 5 years to avoid nexus between management and auditors.

The competent authorities, i.e National Company Law Tribunal/Central Government can take action/s against the unscrupulous professionals on suo moto or on an application made by an aggrieved person.

- Subject to the provisions of this Chapter, every company shall, at the first annual general meeting, appoint an individual or a firm as an auditor who shall hold office from the conclusion of that meeting till the conclusion of its sixth annual general meeting and thereafter till the conclusion of every sixth meeting and the manner and procedure of selection of auditors by the members of the company at such meeting shall be such as may be prescribed:
- No listed company or a company belonging to such class or classes of companies as may be prescribed shall appoint or re-appoint-

(a) an individual as auditor for more than one term of five consecutive years; and

(b) an audit firm as auditor for more than two terms of five consecutive years:

Provided that--

(i) an individual auditor who has completed his term under clause (a) shall not be eligible for re-appointment as auditor in the same company for five years from the completion of his term;

(ii) an audit firm which has completed its term under clause (b), shall not be eligible for reappointment as an auditor in the same company for five years from the completion of such term;

- Comptroller and Auditor General is entrusted with the power to appoint an auditor in Government Companies within 180 days of the commencement of the financial year.
- First auditor other than in government companies to be appointed by the board of directors within 30 days from the date of incorporation failing which members in 90 days by the extraordinary general meeting and the first auditor to be an auditor till the conclusion of the first annual general meeting.

- In the case of government companies, Comptroller and Auditor General will appoint the first auditor within 60 days from the date of incorporation failing which board of directors in the next 30 days and failing which members in the next 60 days, and the auditor will hold office till the conclusion of the first annual general meeting.
- Casual Vacancy of the auditor not appointed by the Comptroller and Auditor General to be filled up by the board of directors within 30 days, and if the vacancy is due to resignation by members, then within 3 months of board recommendation.

### (4) Stringent Penalties on Auditors

The new Act also imposes penalties on the new Independent Professionals'. While in the case of contravention of an auditor's duties, the penalty for the auditor has been made more stringent, if any partners of the audit firm or audit firms has or have acted fraudulently, they shall also be punishable for fraud, fraudulently means to do a thing with an intent to defraud someone under Sec. 447.

### (5) Carrying on of business fraudulently or for unlawful purposes: Sec 206

The Registrar has been empowered to call for information, explanation of documents, or inspect books of the company, either based on information available with him or furnished to him or on a representation given to him by any person if the business of the company is carried on for fraudulent or unlawful purposes.

Calling of information and opportunity of being heard if the business of the company is carried for an unlawful purpose -Sec. 206(4)

The Central Government may, if it is satisfied that the circumstances so warrant, direct the Registrar or an inspector appointed by it for the purpose to carry out the inquiry under this subsection.

Where the business of a company has been or is being carried on for a fraudulent or unlawful purpose, every officer of the company who is in default shall be punishable for fraud in the manner as provided in section 447.

The Central Government may, if it is satisfied that the circumstances so warrant, direct inspection of books and papers of a company by an inspector appointed by it for the purpose. Sec 206(5)

Example

It is seen that many of the companies which are formed for manufacturing or trading activities are running their businesses as NBFC or capital market traders defrauding the investors and these types of companies are taking the benefit of other object clauses of the memorandum of association of the company.

(6) Inspection/Inquiry and investigation into the company's affairs: Sec. 213

The Central Government shall appoint one or more competent persons as inspectors to investigate the affairs of the company.

If after investigation, it is found that the company was formed with a fraudulent or unlawful purpose or the business was conducted to defraud its members, creditors, or any other person concerned in the formation of the company, then every officer who is in default or any other person concerned in the formation of the company and managing its affairs be punishable for fraud under Section 447.

The application can be filed to a Company Law Board, now the National Company Law Tribunal by 100 members or by those members who hold at least 10 percent of the total voting power. The Central Government can appoint inspectors for investigation if the business is conducted with the intent to defraud its members or creditors.

Failure in the finalization of accounts and no annual general meeting being held during that period is a sufficient ground to investigate the affairs of the company.

### (7) Furnishing false statement/ Mutilation/ Destruction of documents: Sec 229

A new section 229 has been added to the Companies Act which provides punishment per Section 447 to such person who, during the course of an inspection, investigation, or inquiry, furnishes any

false statement, or mutilates, destroys, conceals, tampers with, or removes any document relating to a property, assets of affairs of the company.

### (8) Fraudulent Removal of Name: Sec 251

When the Registrar finds that an application for removal of the name of a company (voluntarily striking off of the name) has been filed to evade liabilities of the company or with an intent 10 defraud its creditors or any person(s), then the person in charge of the management of the company shall be liable for punishment under Section 447.

Such person(s) shall also be liable to the person(s) who incurred loss or damages due to the dissolution of the company.

A fake creditor is created, and an application by that fake creditor is moved in the court for winding up of the company. During the process, assets are removed from the site. The original creditor lost his money due to the winding up of the company as no representative appears before the court. The company in order an get an ex-parte order never appears before the court.

### (9) Damages against Delinquent Directors: Section 266(1)

Section 266(1) empowers the Tribunal to assess the damages against delinquent directors during scrutiny or implementation of a scheme of a sick company.

If the tribunal finds that any person, who took part in the formation, promotion, or managing the affairs of such company has misapplied money or property of such company or is found guilty of any misfeasance concerning a sick company, such a person shall be punishable under Section 447.

During the scheme of rehabilitation of a sick company, if Board for Industrial and Financial Reconstruction (now National Company Law Tribunal) finds any person concerned with the promotion, formation, or management of a sick company, has misapplied or retained any money or property of a sick company, then it may direct him to repay or restore the money or property, so misapplied or retained or accountable. It may also direct to compensate the company by any person who took part in the promotion, formation, or management of the Sick Industrial Company.

The authority can also direct banks/financial institutions not to grant any financial assistance for 10 years to any director, officer, or any employee of a sick company who was guilty of divesting the assets of a sick company.

It can also direct bank/financial institutions not to give any financial assistance to any firm or companies in which the above guilty person is proprietor, partner, or director. The said people are criminally liable for misfeasance or wrongful dealing with assets of the sick company.

### (10) Fraudulent Conduct of Business:

During the winding up of the company, if it appears that any business of the company has been carried out to defraud creditors or any other person or for fraudulent purposes, then every person who was knowingly a party to the carrying off of the business shall be liable for action under Section 447.

The Tribunal on the application of the Official Liquidator, Company Liquidator, any creditor or contributory of the company can declare such a person liable personally for debts or other liability of the company.

### (11) False Statement

If any person makes a statement, in any return, report certificate, financial statement, prospectus, statement, or other document required by, or, for, the purposes of this Act, or rules thereunder, which is false or omit any material fact, shall be punishable for fraud under Section 447. Under this section

#### *Section 448: Punishment for false statement*

Save as otherwise provided in this Act, if in any return, report certificate, financial statement, prospectus, statement, or other document required by, or for, the purposes of any of the provisions of this Act or the rules made thereunder, any person makes a statement, mens-rea is important and in the absence of mens-rea, the person cannot be prosecuted.

(a) which is false in any material particulars, knowing it to be false; or

(b) which omits any material fact, knowing it to be material,

he shall be liable under Section 447.

A prospectus which stated that every director had paid share money when two of them had not done, so there is a false statement and attracts the penalty under Section 448 of the Companies Act, 2013.

Penalty for Fraud

Any person, who is found guilty of fraud, shall be punishable with imprisonment for a minimum period of 6 months, which may extend to 10 years, and also a fine equivalent to the amount involved in the fraud, which may extend to three times the amount involved in the fraud.

However, where the fraud involves public interest, the imprisonment shall be for a minimum period of three years.

## 10.5 Oppression and Mismanagement

Oppression involves at least one element of lack of fair dealing of the company against the members as their property rights as shareholders. Mis-management involves the conducting of affairs of the company in a manner prejudicial to its interest.

Sec 241: Application to Tribunal for relief in cases of oppression

It provides that the members of a company can apply to the National Company Law Tribunal for appropriate relief subject to Section 244 against the affairs of the company which is being conducted oppressive to any member

Who can apply to Tribunal in case of oppression and mis-management:

Sec 244: Right to apply under Sec 241

Section 244 (1) The following members of a company shall have the right to apply under Section 241, namely: -

(a) in the case of a company having a share capital, not less than one hundred members of the company or not less than one-tenth of the total number of its members, whichever is less, or any member or members holding not less than one-tenth of the issued share capital of the company, subject to the condition that the applicant of applicants has or have paid all calls and other sums due on his or their shares;

(b) in the case of a company not having a share capital, not less than one-fifth of the total number of its members:

### Appeal to Appellate Tribunal

(1) Any person aggrieved by an order of the Tribunal may prefer an appeal to the Appellate Tribunal.

(2) No appeal shall lie to the Appellate Tribunal from an order made by the Tribunal with the consent of parties

(3) Every appeal under sub-section (1) shall be filed within forty-five days from the date on which a copy of the order of the Tribunal is made available to the person aggrieved and shall be in such form, and accompanied by such fees, as may be prescribed Appellate Tribunal is empowered to extend this period of appeal by another 45 days.

Provided that the Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days from the date aforesaid, but within a further period not exceeding forty- five days, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within that period.

(4) On the receipt of an appeal under sub-section (1), the Appellate Tribunal shall, after giving the parties to the appeal a reasonable opportunity of being heard, pass such orders, thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

### Inspection and Investigation of Books of Accounts by Registrar of Companies/Central Government/SEBI/SFIO

As provided under Section 210 to 222 of the Companies Act, 2013, an investigation into the affairs of companies can be done. A separate process of inspection of Books of Accounts of companies is provided under Sections 206, 207, and 208.

### Relevant provisions of the Securities and Exchange Board of India Act, 1992

The Securities and Exchange Board of India is the regulator of the securities market in India. It was established in the year 1988 and given statutory powers on 12th April 1992 through the SEBI Act, 1992. The SEBI Act, 1992 is "an Act to provide for the establishment of a Board to protect the interests of investors in securities and to promote the interests of investors in securities and to promote the development of, and to regulate the securities market and for matters connected therein or incidental thereto".

The relevant sections dealing with curbing or preventing corporate frauds and their inter-related are discussed below:

## 10.6 Section 11C: Investigation

(1) Where the Board has reasonable ground to believe that---

(a) the transactions in securities are being dealt with in a manner detrimental to the investors or the securities market; or

(b) any intermediary or any person associated with the securities market has violated any of the provisions of this Act or the rules or the regulations made or directions issued by the Board thereunder, it may, at any time by order in writing, direct any person (hereafter in this section referred to as the Investigating Authority) specified in the order to investigate the affairs of such intermediary or persons associated with the securities market and to report thereon to the Board.

(2) Without prejudice to the provisions of sections 235 to 241 of the Companies Act, 1956 (1 of 1956), it shall be the duty of every manager, managing director, officer, and other employee of the company and every intermediary referred to in section 12 or every person associated with the securities market to preserve and to produce to the Investigating Authority or any person authorized by it in this behalf, all the books, registers, other documents and record of, or relating to, the company or, as the case may be, of or relating to, the intermediary or such person, which are in their custody or power.

(3) The Investigating Authority may require any intermediary or any person associated with securities market in any manner to furnish such information to, or produce such books, or registers, or other documents, or record before it or any person authorized by it in this behalf as it may consider necessary if the furnishing of such information or the production of such books, or registers, or other documents, or record is relevant or necessary for the purposes of its investigation.

(4) The Investigating Authority may keep in its custody any books, registers, other documents and record produced under sub-section (2) or sub-section (3) for six months and thereafter shall return the same to any intermediary or any person associated with securities market by whom or on whose behalf the books, registers, other documents and record are produced:

Provided that the Investigating Authority may call for any book, register, other document and record if they are needed again:

Provided further that if the person on whose behalf the books, registers, other documents and record are produced requires certified copies of the books, registers, other documents and record produced before the Investigating Authority, it shall give certified copies of such books, registers, other documents and record to such person or on whose behalf the books, registers, other documents and record were produced.

(5) Any person, directed to make an investigation under sub-section (1), may examine on oath, any manager, managing director, officer and other employee of any intermediary or any person associated with securities market in any manner, in relation to the affairs of his business and may administer an oath accordingly and for that purpose may require any of those persons to appear before it personally.

(6) If any person fails without reasonable cause or refuses--

(a) to produce to the Investigating Authority or any person authorised by it in this behalf any book, register, other document and record which is his duty under sub-section (2) or sub-section (3) to produce; or

(b) to furnish any information which is his duty under sub-section (3) to furnish; or

(c) to appear before the Investigating Authority personally when required to do so under sub-section (5) or to answer any question which is put to him by the Investigating Authority in pursuance of that sub-section; or

(d) to sign the notes of any examination referred to in sub-section (7),

he shall be punishable with imprisonment for a term which may extend to one year, or with fine, which may extend to one crore rupees, or with both, and also with a further fine which may extend to five lakh rupees for every day after the first during which the failure or refusal continues.

## 10.7 Section 11D: Cease and Desist Proceedings

If the Board finds, after causing an inquiry to be made, that any person has violated, or is likely to violate, any provisions of this Act, or any rules or regulations made thereunder, it may pass an order requiring such person to cease and desist from committing or causing such violation:

Provided that the Board shall not pass such order in respect of any listed public company or a public company (other than the intermediaries specified under section 12) which intends to get its securities listed on any recognized stock exchange unless the Board has reasonable grounds to believe that such company has indulged in insider trading or market manipulation.

## 10.8 Section 12: Registration of Stock-Brokers, Sub-Brokers, Share Transfer Agents, etc.

(1) No stock-broker, sub-broker, share transfer agent, banker to an issue, trustee of a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and such other intermediary who may be associated with the securities market shall buy, sell or deal in securities except under, and in accordance with, the conditions of a certificate of registration obtained from the Board in accordance with the regulations made under this Act:

Proviso 1: Intermediaries working before SEBI Act have to obtain a Registration Certificate within 3 months

Proviso 1: No new Registration certificate if certificate is obtained under Securities Laws (Amendment) Act, 1995

(1A) No depository, participant, custodian of securities, foreign institutional investor, credit rating agency or any other intermediary associated with the securities market as the Board may by notification in this behalf specify, shall buy or sell or deal in securities except under and in accordance with the conditions of a certificate of registration obtained from the Board in accordance with the regulations made under this Act:

(1B) No person shall sponsor or cause to be sponsored or carry on or cause to be carried on any venture capital funds or collective investment scheme including mutual funds, unless he obtains a certificate of registration from the Board in accordance with the regulations:

(IC) No person shall sponsor or cause to be sponsored or carry on or cause to be carried on the activity of an alternative investment fund or a business trust as defined in clause (13A) of section 2 of the Income-tax Act, 1961 (43 of 1961), unless a certificate or registration is granted by the Board in accordance with the regulations made under this Act.

(2) Every application for registration shall be in such manner and on payment of such fees as may be determined by regulations.

(3) The Board may, by order, suspend or cancel a certificate of registration in such manner as may be determined by regulations:

Provided that no order under this sub-section shall be made unless the person concerned has been given a reasonable opportunity of being heard.

## 10.9 Section 12A: Prohibition of Manipulative and Deceptive Devices, Insider Trading and Substantial Acquisition of Securities or Control.

No person shall directly or indirectly--

(a) use or employ, in connection with the issue, purchase or sale of any securities listed or proposed to be listed on a recognized stock exchange, any manipulative or deceptive device or contrivance in contravention of the provisions of this Act or the rules or the regulations made thereunder;

(b) employ any device, scheme or artifice to defraud in connection with issue or dealing in securities which are listed or proposed to be listed on a recognized stock exchange;

(c) engage in any act, practice, course of business which operates or would operate as fraud or deceit upon any person, in connection with the issue, dealing in securities which are listed or proposed to be listed on a recognized stock exchange, in contravention of the provisions of this Act or the rules or the regulations made thereunder;

(d) engage in insider trading;

(e) deal in securities while in possession of material or non-public information or communicate such material or non-public information to any other person, in a manner which is in contravention of the provisions of this Act or the rules or the regulations made thereunder;

(f) acquire control of any company or securities more than the percentage of equity share capital of a company whose securities are listed or proposed to be listed on a recognized stock exchange in contravention of the regulations made under this Act.

## 10.10 Section 15A: Penalty for Failure to Furnish Information, Return, etc.

If any person, who is required under this Act or any rules or regulations made thereunder, ---

(a) to furnish any document, return or report to the Board, fails to furnish the same, or who furnishes or files false, incorrect or incomplete information, return, report, books or other documents, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(b) to file any return or furnish any information, books, or other documents within the time specified therefor in the regulations, fails to file the return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(c) to maintain books of account or records fails to maintain the same, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.11 Section 15B: Penalty for Failure by any Person to Enter into Agreement with Clients

If any person, who is registered as an intermediary and is required under this Act or any rules or regulations made thereunder to enter into an agreement with his client, fails to enter into such agreement, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.12 Section 15C: Penalty for Failure to Redress Investors' Grievances

If any listed company or any person who is registered as an intermediary, after having been called upon by the Board in writing including by any means of electronic communication, to redress the grievances of investors, fails to redress such grievances within the time specified by the Board, such company or intermediary shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.13 Section 15D: Penalty for Certain Defaults in Case of Mutual Funds

If any person, who is---

(a) required under this Act or any rules or regulations made thereunder to obtain a certificate of registration from the Board for sponsoring or carrying on any collective investment scheme, including mutual funds, sponsors or carries on any collective investment scheme, including mutual funds, without obtaining such certificate of registration, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which he sponsors or carries on any such collective investment scheme including mutual funds subject to a maximum of one crore rupees;

(b) registered with the Board as a collective investment scheme, including mutual funds, for sponsoring or carrying on any investment scheme, fails to comply with the terms and conditions of certificate of registration, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(c) registered with the Board as a collective investment scheme including mutual funds, fails to make an application for listing of its schemes as provided for in the regulations governing such listing, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(d) registered as a collective investment scheme, including mutual funds, fails to despatch unit certificates of any scheme in the manner provided in the regulation governing such despatch, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(e) registered as collective investment scheme, including mutual funds, fails to refund the application monies paid by the investors within the period specified in the regulations, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees;

(f) registered as a collective investment scheme, including mutual funds, fails to invest money collected by such collective investment schemes in the manner or within the period specified in the regulations, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.14 Section 15E: Penalty for Failure to Observe Rules and Regulations by an Asset Management Company

Where any asset management company of a mutual fund registered under this Act fails to comply with any of the regulations providing for restrictions on the activities of the asset management companies, such asset management company shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.15 Section 15EA: Penalty for Default in Case of Alternative Investment Funds, Infrastructure Investment Trusts and Real Estate Investment Trusts

Where any person fails to comply with the regulations made by the Board in respect of alternative investment funds, infrastructure investment trusts and real estate investment trusts or fails to comply with the directions issued by the Board, such person shall be liable to penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees or three times the amount of gains made out of such failure, whichever is higher.

## 10.16 Section 15EB: Penalty for Default in Case of Investment Adviser and Research Analyst

Where an investment adviser or a research analyst fails to comply with the regulations made by the Board or directions issued by the Board, such investment adviser or research analyst shall be liable to penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which such failure continues subject to a maximum of one crore rupees.

## 10.17 Section 15F: Penalty for Default in Case of Stock Brokers

If any person, who is registered as a stock broker under this Act, ---

(a) fails to issue contract notes in the form and manner specified by the stock exchange of which such broker is a member, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one crore rupees for which the contract note was required to be issued by that broker;

(b) fails to deliver any security or fails to make payment of the amount due to the investor in the manner within the period specified in the regulations, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to one lakh rupees for each day during which6[such failure continues] subject to a maximum of one crore rupees;

(c) charges an amount of brokerage which is in excess of the brokerage specified in the regulations, he shall be liable to a penalty which shall not be less than one lakh rupees but which may extend to five times the amount of brokerage charged in excess of the specified brokerage, whichever is higher.

## 10.18 Section 15G: Penalty for Insider Trading

If any insider who,

(i) either on his own behalf or on behalf of any other person, deals in securities of a body corporate listed on any stock exchange on the basis of any unpublished price sensitive information; or

(ii) communicates any unpublished price sensitive information to any person, with or without his request for such information except as required in the ordinary course of business or under any law; or

(iii) counsels, or procures for any other person to deal in any securities of anybody corporate on the basis of unpublished price sensitive information,

shall be liable to a penalty which shall not be less than ten lakh rupees but which may extend to twenty-five crore rupees or three times the amount of profits made out of insider trading, whichever is higher.

## 10.19 Section 15H: Penalty for non-disclosure of acquisition of shares and takeovers

If any person, who is required under this Act or any rules or regulations made thereunder, fails to

(i) disclose the aggregate of his shareholding in the body corporate before he acquires any shares of that body corporate; or

(ii) make a public announcement to acquire shares at a minimum price;

(iii) make a public offer by sending letter of offer to the shareholders of the concerned company; or

(iv) make payment of consideration to the shareholders who sold their shares pursuant to letter of offer,

he shall be liable to a penalty which shall not be less than ten lakh rupees but which may extend to twenty-five crore rupees or three times the amount of profits made out of such failure, whichever is higher.

**Task:**If an individual or firm indulges in fraudulent and unfair trade practices relating to securities, will he/she/it get any penalty under the SEBI Act, 1992? [Hint: Section 15HA]

**Task:** If any person knowingly alters or destroys any information, record, or document (including electronic records), which is required under this SEBI Act or any rules or regulations made there under, to obstruct the investigation of any matter within the jurisdiction of the Board, How will he be penalized? [Hint: Section 15HAA]

## 10.20 Section 15HB: Penalty for Contravention Where No Separate Penalty Has Been Provided

Whoever fails to comply with any provision of this Act, the rules or the regulations made or directions issued by the Board thereunder for which no separate penalty has been provided, shall be liable to a penalty which shall not be less one lakh rupees but which may extend to one crore rupees.

## 10.21 Section 15K: Establishment of Securities Appellate Tribunals

(1) The Central Government shall, by notification, establish a Tribunal to be known as the Securities Appellate Tribunal to exercise the jurisdiction, powers and authority conferred on it by or under this Act or any other law for the time being in force.

(2) The Central Government shall also specify in the notification referred to in sub-section (1), the matters and places in relation to which the Securities Appellate Tribunal may exercise jurisdiction.

## 10.22 Section 15L: Composition of Securities Appellate

The Securities Appellate Tribunal shall consist of a Presiding Officer and such number of Judicial Members and Technical Members as the Central Government may determine, by notification, to exercise the powers and discharge the functions conferred on the Securities Appellate Tribunal under this Act or any other law for the time being in force.

(2) Subject to the provisions of this Act,

(a) the jurisdiction of the Securities Appellate Tribunal may be exercised by Benches thereof;

(b) a Bench may be constituted by the Presiding Officer of the Securities Appellate Tribunal with two or more Judicial or Technical Members as he may deem fit:

Provided that every Bench constituted shall include at least one Judicial Member and one Technical Member;

(c) the Benches of the Securities Appellate Tribunal shall ordinarily sit at Mumbai and may also sit at such other places as the Central Government may, in consultation with the Presiding Officer, notify.

(3) Notwithstanding anything contained in sub-section (2), the Presiding Officer may transfer a Judicial Member or a Technical Member of the Securities Appellate Tribunal from one Bench to another Bench.

## 10.23 Section 15T: Appeal to the Securities Appellate Tribunal

Save as provided in sub-section (2), any person aggrieved, --

(a) by an order of the Board made, on and after the commencement of the Securities Laws (Second Amendment) Act, 1999 (32 of 1999), under this Act, or the rules or regulations made thereunder; or

(b) by an order made by an adjudicating officer under this Act; or

(c) by an order of the Insurance Regulatory and Development Authority or the Pension Fund Regulatory and Development Authority, may prefer an appeal to a Securities Appellate Tribunal having jurisdiction in the matter.

(3) Every appeal under sub-section (1) shall be filed within forty-five days from the date on which a copy of the order made by the Board or the adjudicating officer or the Insurance Regulatory and Development Authority or the Pension Fund Regulatory and Development Authority as the case may be, is received by him and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Securities Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Securities Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Securities Appellate Tribunal shall send a copy of every order made by it to the Board, or the Insurance Regulatory and Development Authority or the Pension Fund Regulatory and Development Authority, as the case may be the parties to the appeal and to the concerned adjudicating officer.

(6) The appeal filed before the Securities Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

## 10.24 Section15Y: Civil Court not to have jurisdiction

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudication officer appointed under this Act or a Securities Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**Section 15Z. Appeal to Supreme Court**

Any person aggrieved by any decision or order of the Securities Appellate Tribunal may file an appeal to the Supreme Court within sixty days from the date of communication of the decision or order of the Securities Appellate Tribunal to him on any question of law arising out of such order:

Provided that the Supreme Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

## 10.25 Section 23: Protection of Action Taken in Good Faith

No suit, prosecution or other legal proceedings shall lie against the Central Government or Board or any officer of the Central Government or any member, officer or other employee of the Board for anything which is in good faith done or intended to be done under this Act or the rules or regulations made thereunder.

## 10.26 Section 24: Offences

(1) Without prejudice to any award of penalty by the adjudicating officer or the Board under this Act, if any person contravenes or attempts to contravene or abets the contravention of the provisions of this Act or of any rules or regulations made thereunder, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine, which may extend to twenty-five crore rupees or with both.

(2) If any person fails to pay the penalty imposed by the adjudicating officer or the Board or fails to comply with any directions or orders, he shall be punishable with imprisonment for a term which shall not be less than one month but which may extend to ten years, or with fine, which may extend to twenty-five crore rupees or with both.

Task

Discuss the consequences of committing an offense by a company. [Hint: Section 27]

## Summary

The legal environment plays a crucial role in determining the nature of corporate governance. The two important aspects of corporate fraud are: (1) de jure protection the protection offered under the laws and (2) de facto protection-the extent to which the laws have been enforced.

Many sections of the Companies Act, 2013 and the SEBI Act, 1992 focus on curbing and preventing fraud in the country.

Sections 7(5), 7(6), 8(11), 34, 36, 38(1),46(5), 56(7), 66(10), 75(1), 132, 139, 140(5), 206, 207, 208, 209, 210, 211, 212, 213, 216, 217, 219, 220, 221, 222, 223, 224, 229, 241, 244, 251(1), 266(1), 339(3), 447, and 448 of the Companies Act, 2013 are relevant sections in the context of fraud prevention.

National Company Law Appellant Tribunal followed by High courts are the Redressal Authorities under the Companies Act, 2013.

Section 11, 11C, 11D, 12, 12A, 15A, 15B, 15C, 15D, 15E, 15F, 15G, 15H, 15HA, 15HB, 15K, 15L, 15R, 15T, 15V, 15Y, 15Z, 20, 23, 24, 24A and 27 of the SEBI Act,1992 are relevant sections in the context of fraud prevention.

The Securities Appellate Tribunal followed by Supreme Court is the Redressal Authorities under the SEBI Act, 1992.

## Keywords

Accounting standards: These means the standards of accounting or any addendum thereto for companies or class of companies referred to in section 133.

Alter: "Alter" or "alteration" includes the making of additions, omissions, and substitutions.

Appellate Tribunal: It means the National Company Law Appellate Tribunal constituted under section 410 of the Companies Act, 2013 and the Securities Appellate Tribunal constituted under Section 15K of the SEBI Act, 1992.

Company: It means anybody corporate and includes a firm or other association of individuals.

Contributory: It means a person liable to contribute towards the assets of the company in the event of its being wound up.

Director: Concerning a firm, means a partner in the firm.

Fraud: Concerning affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

Officer: It includes any director, manager or key managerial personnel, or any person under whose directions or instructions the Board of Directors or any one or more of the directors is or are accustomed to act

Securities: It has the meaning assigned to it in section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956).

Wrongful gain: It means the gain by unlawful means of property to which the person gaining is not legally entitled

Wrongful loss: It means the loss by unlawful means of property to which the person losing is legally entitled.

## Self Assessment

1. Which one of the following is the enforcement authority under the Companies Act, 2013?

A. Civil Courts

B. The Securities and Exchange Board of India

C. Registrar of Companies

D. District and Sessions Court

2. Which one of the following is the enforcement authority under the Benami Transactions (Prohibition) Act, 1988?

A. Civil Courts

B. SEBI

C. ROC

D. NCLT

3. Which one of the following is the enforcement authority under the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974?

A. State Government

B. Central Government

C. State Commission

D. District Commission

4. Which one of the following is the enforcement authority under the Indian Penal Code, 1860?

A. NCLT

B. SEBI

C. RBI

D. District & Sessions Court

5. Which one of the following is the enforcement authority under the Securities and Exchange Board of India Act, 1992?

A. NCLT

B. SEBI

C. RBI

D. District & Sessions Court

6. Any person who is found to be guilty of fraud, involving an amount of at least ten lakh rupees or one percent of the turnover of the company, whichever is lower shall be punishable with:

A. Up to 6 months imprisonment
B. Up to 6 months imprisonment but which may extend to 10 years
C. Fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud
D. Up to 6 months imprisonment but which may extend to 10 years and a fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud

7. A person who makes multiple applications under different names for acquiring or subscribing to securities shall be liable under the following section of the Companies Act, 2013:

A. Section 445
B. Section 446
C. Section 447
D. Section 448

8. If a company issues duplicate share certificates to defraud, then who shall be liable for action under Section 447 of the Act?

A. Company itself
B. Every officer of the company
C. Company and it's every officer
D. Every defaulting officer of the company

9. NFRA stands for:

A. National Foreign Reporting Authority
B. National Financial Reporting Authority
C. National Financial Regulatory Authority
D. National Foreign Regulatory Authority

10. No listed company or a company belonging to such class or classes of companies as may be prescribed shall appoint or re-appoint-

A. an individual as auditor for more than one term of five consecutive years
B. an individual as auditor for more than one term of ten consecutive years
C. an individual as auditor for more than one term of three consecutive years
D. an individual as auditor for more than one term of two consecutive years

11. If any person fails without reasonable cause refuses to furnish any information which is his duty under sub-section (3) to furnish, he shall be punishable with:

A. Imprisonment for up to one year
B. Fine up to one crore rupees
C. Imprisonment for up to one year and Fine up to one crore rupees
D. Imprisonment for up to one year, Fine up to one crore rupees, and a further fine which may extend to five lakh rupees for every day after the first during which the refusal continues

12. Intermediaries working before SEBI Act have to obtain a Registration Certificate within:

A. 1 month
B. 3 months
C. 1 year
D. 3 years

13. If any person, who is required under the SEBI Act, 1992 to furnish any document, return or report to the Board, fails to furnish the same, then he shall be liable for:

A. A penalty of one lakh rupees
B. A penalty of one lakh rupees per day during which such failure continues
C. A penalty of one lakh rupees per day during which such failure continues or one crore rupees whichever is less
D. A penalty of one lakh rupees per day during which such failure continues or one crore rupees whichever is more

14. If any person indulges in insider trading, he shall be liable for:

A. A penalty of ten lakh rupees
B. A penalty of ten lakh rupees or twenty-five crore rupees whichever is higher
C. A penalty of ten lakh rupees or twenty-five crore rupees or three times of profit made from insider training whichever is higher
D. A penalty of ten lakh rupees and twenty-five crore rupees and three times of profit made from insider training

15. Securities Appellate Tribunal has to dispose of the appeal finally within _____ from the receipt of the appeal.

A. Three months
B. Forty-five days
C. Six months
D. Thirty days

## Answers for Self Assessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | C | 2. | A | 3. | B | 4. | D | 5. | B |
| 6. | D | 7. | C | 8. | D | 9. | B | 10. | A |
| 11. | D | 12. | B | 13. | C | 14. | C | 15. | C |

## Review Questions

1. Explain the Penalty for alteration, destruction, etc., of records and failure to protect the electronic database of the Board as per Section 15HAA of SEBI Act, 1992.
2. Explain the provisions related to the establishment and composition of Securities Appellate Tribunals.
3. Discuss the provisions related to putting an appeal to the Securities Appellate Tribunals.

4. Which resolution is available for the person who is aggrieved by the decision of Securities Appellate Tribunals?
5. Write short notes on the following sections of the Companies Act, 2013:
   a. Section 447
   b. Section 36
   c. Section 132
   d. Section 448
6. Discuss relevant sections along with its interrelated provisions related to preventing fraud under the Companies Act, 2013.
7. Discuss relevant sections along with its interrelated provisions related to penalizing fraudsters to deter other fraudsters under the Companies Act, 2013.
8. What is NFRA? Explain the objectives and Powers of NFRA.
9. Explain the sections under the Companies Act, 2013 that deal with the fraudulent raising of share capital along with the penalties for such offenses.
10. Discuss the provisions of Section 11C of the SEBI Act, 1992 in detail.
11. Explain the provisions for registration of stock-brokers, sub-brokers, and share transfer agents.
12. Write short notes on the following sections of the SEBI Act, 1992:
    a. Section 23
    b. Section 24
    c. Section 15G
13. What is insider training? Explain the penalty for insider trading.
14. Who can file an appeal in the Securities Appellate Tribunal? Explain the redressal procedure of the Securities Appellate Tribunal as per Section 15T.

## Further Readings


- Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.


### Web Links

- https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789/1362
- https://www.indiacode.nic.in/handle/123456789/1890?sam_handle=123456789/1362

Dr. Razia Sehdev, Lovely Professional University

# Unit 11: Regulatory Measures for Curbing Corporate Fraud-2

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the meaning of Benami Transactions.
- summarize the relevant provisions of the Benami Transaction (Prohibition) Act, 1988 that deal with curbing corporate fraud in India.
- explain the relevant sections of the Money Laundering Act, 2002 for curbing Corporate Fraud in India.
- summarize the relevant provisions of the Money Laundering Act, 2002 for curbing Corporate Fraud in India.

## Introduction

Benami transactions have been a part of Indian society for a while. However, gradually it was realized that Benami Transactions were being employed for various dishonourable motives, including but not limited to, money laundering and evasion of taxes. It was also realized that these transactions could be misused for diverting one's assets in another's name and thereby defeating the lawful claims of creditors and defrauding them. Slowly and gradually it dawned that, on a cost-benefit analysis, the losses and mischief arising from allowing benami transactions to continue unabated far outweighed their perceived advantages, leading to such transactions being forbidden by law. The present unit discusses a few relevant provisions of the Benami Transaction (Prohibition) Act, 1988.

Money laundering is concealing the origin of money obtained from illegal activities such as drug trafficking, corruption, embezzlement, or gambling and converting the illegal money into a legitimate source. It is an issue in itself. It is dangerous for internal and external security. Money laundering cases include terrorist activities. To prevent these illegal activities, the government of India (GOI) introduced the Prevention of Money Laundering Act (PMLA) in 2002. The present unit discusses a few relevant provisions of the PMLA, 1988 that focuses on curbing fraud cases in the country.

## 11.1 The Prohibition of Benami Property Transactions Act, 1988

The Benami Transaction (Prohibition) Act is "an Act to prohibit benami transactions and the right to recover property held benami for matters connected therewith or incidental thereto."

Section 1:

(1) This Act may be called the Prohibition of Benami Property Transactions Act, 1988.

(2) It extends to the whole of India.

(3) The provisions of sections 3, 5 and 8 shall come into force at once, and the remaining provisions of this Act shall be deemed to have come into force on the 19th day of May, 1988.

### What is Benami Transaction?

A benami transaction means,--

(A) a transaction or an arrangement--

(a) where a property is transferred to, or is held by, a person, and the consideration for such property has been provided, or paid by, another person; and

(b) the property is held for the immediate or future benefit, direct or indirect, of the person who has provided the consideration,

except when the property is held by—(Exceptions)

(i) a Karta, or a member of a Hindu undivided family, as the case may be, and the property is held for his benefit or benefit of other members in the family and the consideration for such property has been provided or paid out of the known sources of the Hindu undivided family;

(ii) a person standing in a fiduciary capacity for the benefit of another person towards whom he stands in such capacity and includes a trustee, executor, partner, director of a company, a depository or a participant as an agent of a depository under the Depositories Act, 1996 (22 of 1996) and any other person as may be notified by the Central Government for this purpose;

(iii) any person being an individual in the name of his spouse or in the name of any child of such individual and the consideration for such property has been provided or paid out of the known sources of the individual;

(iv) any person in the name of his brother or sister or lineal ascendant or descendant, where the names of brother or sister or lineal ascendant or descendant and the individual appear as joint owners in any document, and the consideration for such property has been provided or paid out of the known sources of the individual; or

(B) a transaction or an arrangement in respect of a property carried out or made in a fictitious name; or

(C) a transaction or an arrangement in respect of a property where the owner of the property is not aware of, or, denies knowledge of, such ownership;

(D) a transaction or an arrangement in respect of a property where the person providing the consideration is not traceable or is fictitious;

**Did you know?**

Are Benami Transactions legal?

With an increase in mischievous activities, Benami transactions are deemed to be illegal and unlawful.

The relevant sections that deal with curbing or preventing corporate frauds and the sections inter-related to the relevant sections are:

Section 3: Prohibition of benami transactions

Section 4: Prohibition of the right to recover property held benami

Section 5: Property held benami liable to acquisition

Section 6: Prohibition on re-transfer of property by benamidar

Section 7: Adjudicating Authority

Section 18: Authorities and Jurisdiction

Section 19: Powers of authorities

Section 20: Certain officers to assist in inquiry, etc.

Section 30:Establishment of Appellate Tribunal

Section 53: Penalty for benami transaction

Section 54: Penalty for false information

### Section 3: Prohibition of Benami Transactions

(1) No person shall enter into any benami transaction.

(2) Whoever enters into any benami transaction shall be punishable with imprisonment for a term which may extend to three years or with fine or with both.

(3) Whoever enters into any benami transaction on and after the date of commencement of the Benami Transactions (Prohibition) Amendment Act, 2016 (43 of 2016) shall, notwithstanding anything contained in sub-section (2), be punishable in accordance with the provisions contained in Chapter VII.

### Section 4: Prohibition of the right to recover property held benami

(1) No suit, claim or action to enforce any right in respect of any property held benami against the person in whose name the property is held or against any other person shall lie by or on behalf of a person claiming to be the real owner of such property.

(2) No defence based on any right in respect of any property held benami, whether against the person in whose name the property is held or against any other person, shall be allowed in any suit, claim or action by or on behalf of a person claiming to be the real owner of such property.

### Section 5: Property held benami liable to confiscation

Any property, which is subject matter of benami transaction, shall be liable to be confiscated by the Central Government.

### Section 6: Prohibition on re-transfer of property by benamidar

(1) No person, being a benamidar shall re-transfer the benami property held by him to the beneficial owner or any other person acting on his behalf.

(2) Where any property is re-transferred in contravention of the provisions of sub-section (1), the transaction of such property shall be deemed to be null and void.

(3) The provisions of sub-sections (1) and (2) shall not apply to a transfer made in accordance with the provisions of section 190 of the Finance Act, 2016 (28 of 2016).

### Section 7: Adjudicating Authority

The competent authority authorized under sub-section (1) of section 5 of the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976 (13 of 1976) shall be the Adjudicating Authority to exercise jurisdiction, powers and authority conferred by or under this Act.

### Section 18: Authorities and jurisdiction

(1) The following shall be the authorities for the purposes of this Act, namely:--

(a) the Initiating Officer;

(b) the Approving Authority;

(c) the Administrator; and

(d) the Adjudicating Authority.

(2) The authorities shall exercise all or any of the powers and perform all or any of the functions conferred on, or, assigned, as the case may be, to it under this Act or in accordance with such rules as may be prescribed.

### Section 19: Powers of authorities

(1) The authorities shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit in respect of the following matters, namely:--

(a) discovery and inspection;

(b) enforcing the attendance of any person, including any official of a banking company or a public financial institution or any other intermediary or reporting entity, and examining him on oath;

(c) compelling the production of books of account and other documents;

(d) issuing commissions;

(e) receiving evidence on affidavits; and

(f) any other matter which may be prescribed.

(2) All the persons summoned under sub-section (1) shall be bound to attend in person or through authorized agents, as any authority under this Act may direct, and shall be bound to state the truth upon any subject respecting which they are examined or make statements, and produce such documents as may be required.

(3) Every proceeding under sub-section (1) or sub-section (2) shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 of the Indian Penal Code (45 of 1860).

(4) For the purposes of this Act, any authority under this Act may requisition the service of any police officer or of any officer of the Central Government or State Government or of both to assist him for all or any of the purposes specified in sub-section (1), and it shall be the duty of every such officer to comply with the requisition or direction.

(5) For the purposes of this section, "reporting entity" means any intermediary or any authority or of the Central or the State Government or any other person as may be notified in this behalf.

Explanation.--For the purposes of sub-section (5), "intermediary" shall have the same meaning as assigned to it in clause (n) of sub-section (1) of section 2 of the Prevention of Money-Laundering Act, 2002 (15 of 2003).

### Section 20: Certain officers to assist in inquiry, etc.

The following officers shall assist the authorities in the enforcement of this Act, namely:--

(a) income-tax authorities appointed under sub-section (1) of section 117 of the Income-tax Act, 1961 (43 of 1961);

(b) officers of the Customs and Central Excise Departments;

(c) officers appointed under sub-section (1) of section 5 of the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985);

(d) officers of the stock exchange recognized under section 4 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);

(e) officers of the Reserve Bank of India constituted under sub-section (1) of section 3 of the Reserve Bank of India Act, 1934 (2 of 1934);

(f) police;

(g) officers of enforcement appointed under sub-section (1) of section 36 of the Foreign Exchange Management Act, 1999 (40 of 1999);

(h) officers of the Securities and Exchange Board of India established under section 3 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);

(i) officers of any other body corporate constituted or established under a Central or a State Act; and

(j) such other officers of the Central Government, State Government, local authorities or banking companies as the Central Government may, by notification, specify, in this behalf.

### Section 30: Establishment of Appellate Tribunal

The Central Government shall, by notification, establish an Appellate Tribunal to hear appeals against the orders of any authority under this Act.

### Section 53: Penalty for benami transaction

(1) Where any person enters into a benami transaction in order to defeat the provisions of any law or to avoid payment of statutory dues or to avoid payment to creditors, the beneficial owner, benamidar and any other person who abets or induces any person to enter into the benami transaction, shall be guilty of the offence of benami transaction.

(2) Whoever is found guilty of the offence of benami transaction referred to in sub-section (1) shall be punishable with rigorous imprisonment for a term which shall not be less than one year, but which may extend to seven years and shall also be liable to fine which may extend to twenty-five per cent of the fair market value of the property.

### Section 54: Penalty for false information

Any person who is required to furnish information under this Act knowingly gives false information to any authority or furnishes any false document in any proceeding under this Act, shall be punishable with rigorous imprisonment for a term which shall not be less than six months but which may extend to five years and shall also be liable to fine which may extend to ten per cent of the fair market value of the property.

## 11.2 The Money Laundering Act, 2002

The Money Laundering Act is "an Act to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money laundering and for matters connected therewith or incidental thereto".

It extends to the whole of India.

The Prevention of Money Laundering Act, 2002 (PMLA), forms the core of the legal framework in India to combat 'money laundering'.

The relevant sections and their inter-related sections to curb fraud are discussed below:

### Section 3: Offence of money-laundering

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of the offence of money-laundering.

Explanation.--For the removal of doubts, it is hereby clarified that,--

(i) a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:--

(a) concealment; or

(b) possession; or

(c) acquisition; or

(d) use; or

(e) projecting as untainted property; or

(f) claiming as untainted property,

in any manner whatsoever;

(ii) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.

### Section 4: Punishment for money-laundering

Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine:

Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted.

### Section 12: Reporting entity to maintain records

(1) Every reporting entity shall--

(a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;

(b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;

(e) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

Caution: Clauses (c) and (d) omitted by Act 14 of 2019, s. 28 (w.e.f. 25-07-2019).

### Section 12A: Access to information

(1) The Director may call for from any reporting entity any of the records referred to in section 11A, sub-section (1) of section 12, sub-section (1) of section 12AA and any additional information as he considers necessary for the purposes of this Act.

(2) Every reporting entity shall furnish to the Director such information as may be required by him under sub-section (1) within such time and in such manner as he may specify.

(3) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section (1), shall be kept confidential.

### Section 13: Powers of Director to impose fine

(1) The Director may, either of his own motion or on an application made by any authority, officer or person, make such inquiry or cause such inquiry to be made, as he thinks fit to be necessary, with regard to the obligations of the reporting entity, under this Chapter.

(1A) If at any stage of inquiry or any other proceedings before him, the Director having regard to the nature and complexity of the case, is of the opinion that it is necessary to do so, he may direct the concerned reporting entity to get its records, as may be specified, audited by an accountant from amongst a panel of accountants, maintained by the Central Government for this purpose.

(1B)The expenses of, and incidental to, any audit under sub-section (1A) shall be borne by the Central Government.

(2) If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may--

(a) issue a warning in writing; or

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

(3) The Director shall forward a copy of the order passed under sub-section (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section.

### Section 15: Procedure and manner of furnishing information by reporting entities

The Central Government may, in consultation with the Reserve Bank of India, prescribe the procedure and the manner of maintaining and furnishing information by a reporting entity under section 11A, sub-section (1) of section 12 and sub-section (1) of section 12AA to implement the provisions of this Act.

### Section 17: Search and seizure

(1) Where the Director or any other officer not below the rank of Deputy Director authorized by him for this section, based on information in his possession, has reason to believe (the reason for such belief to be recorded in writing) that any person--

(i) has committed any act which constitutes money-laundering, or

(ii) is in possession of any proceeds of crime involved in money-laundering, or

(iii) is in possession of any records relating to money-laundering, [or]

(iv) is in possession of any property related to crime,

then, subject to the rules made in this behalf, he may authorize any officer subordinate to him to--

(a) enter and search any building, place, vessel, vehicle or aircraft where he has reason to suspect that such records or proceeds of crime are kept;

(b) break open the lock of any door, box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (a) where the keys thereof are not available;

(c) seize any record or property found as a result of such search;

(d) place marks of identification on such record or property, if required or make or cause to be made extracts or copies therefrom;

(e) make a note or an inventory of such record or property;

(f) examine on oath any person, who is found to be in possession or control of any record or property, in respect of all matters relevant for the purposes of any investigation under this Act:

(1A) Where it is not practicable to seize such record or property, the officer authorized under sub-section (1), may make an order to freeze such property whereupon the property shall not be transferred or otherwise dealt with, except with the prior permission of the officer making such order, and a copy of such order shall be served on the person concerned:

Provided that if, at any time before its confiscation under sub-section (5) or sub-section (7) of section 8 or section 58B or sub-section (2A) of section 60, it becomes practical to seize a frozen property, the officer authorized under sub-section (1) may seize such property.

(2) The authority, who has been authorized under sub-section (1) shall, immediately after search and seizure or upon issuance of a freezing order], forward a copy of the reasons so recorded along with material in his possession, referred to in that sub-section, to the Adjudicating Authority in a sealed envelope, in the manner, as may be prescribed and such Adjudicating Authority shall keep such reasons and material for such period, as may be prescribed.

(3) Where an authority, upon information obtained during survey under section 16, is satisfied that any evidence shall be or is likely to be concealed or tampered with, he may, for reasons to be recorded in writing, enter and search the building or place where such evidence is located and seize that evidence:

Provided that no authorization referred to in sub-section (1) shall be required for search under this sub-section.

(4) The authority seizing any record or property under sub-section (1) or freezing any record or property under sub-section (1A) shall, within a period of thirty days from such seizure or freezing, as the case may be, file an application, requesting for retention of such record or property seized

under sub-section (1) or for continuation of the order of freezing served under sub-section (1A), before the Adjudicating Authority.

### Section 19: Power to arrest

(1) If the Director, Deputy Director, Assistant Director or any other officer authorized in this behalf by the Central Government by general or special order, has based on material in his possession, reason to believe (the reason for such belief to be recorded in writing) that any person has been guilty of an offence punishable under this Act, he may arrest such person and shall, as soon as may be, inform him of the grounds for such arrest.

(2) The Director, Deputy Director, Assistant Director or any other officer shall, immediately after arrest of such person under sub-section (1), forward a copy of the order along with the material in his possession, referred to in that sub-section, to the Adjudicating Authority in a sealed envelope, in the manner, as may be prescribed and such Adjudicating Authority shall keep such order and material for such period, as may be prescribed.

(3) Every person arrested under sub-section (1) shall, within twenty-four hours, be taken to a Special Court or Judicial Magistrate or a Metropolitan Magistrate, as the case may be, having jurisdiction:

Provided that the period of twenty-four hours shall exclude the time necessary for the journey from the place of arrest to the Special Court or Magistrate's Court.

### Section 24: Burden of proof

In any proceeding relating to proceeds of crime under this Act,--

(a) in the case of a person charged with the offence of money-laundering under section 3, the Authority or Court shall, unless the contrary is proved, presume that such proceeds of crime are involved in money-laundering; and

(b) in the case of any other person the Authority or Court, may presume that such proceeds of crime are involved in money-laundering.

### Section 25: Appellate Tribunal

The Appellate Tribunal constituted under sub-section (1) of section 12 of the Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976 (13 of 1976) shall be the Appellate Tribunal for hearing appeals against the orders of the Adjudicating Authority and the other authorities under this Act.

### Section 26: Appeal to Appellate Tribunal

(1) Save as otherwise provided in sub-section (3), the Director or any person aggrieved by an order made by the Adjudicating Authority under this Act, may prefer an appeal to the Appellate Tribunal.

(2) Any reporting entity aggrieved by any order of the Director made under sub-section (2) of section 13, may prefer an appeal to the Appellate Tribunal.

(3) Every appeal preferred under sub-section (1) or sub-section (2) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Adjudicating Authority or Director is received and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Appellate Tribunal may, after giving an opportunity of being heard, entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1) or sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Adjudicating Authority or the Director, as the case may be.

(6) The appeal filed before the Appellate Tribunal under sub-section (1) or sub-section (2) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of filing of the appeal.

### Section 42: Appeal to High Court

Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of law or fact arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

**Task:** Discuss Special Courts under the Money Laundering Act, 2002. [Hint: Section 43]

### Section 66: Disclosure of information

(1) The Director or any other authority specified by him by a general or special order in this behalf may furnish or cause to be furnished to--

(i) any officer, authority or body performing any functions under any law relating to imposition of any tax, duty or cess or to dealings in foreign exchange, or prevention of illicit traffic in the narcotic drugs and psychotropic substances under the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985); or

(ii) such other officer, authority or body performing functions under any other law as the Central Government may, if in its opinion it is necessary so to do in the public interest, specify, by notification in the Official Gazette, in this behalf, any information received or obtained by such Director or any other authority, specified by him in the performance of their functions under this Act, as may, in the opinion of the Director or the other authority, so specified by him, be necessary for the purpose of the officer, authority or body specified in clause (i) or clause (ii) to perform his or its functions under that law.

(2) If the Director or other authority specified under sub-section (1) is of the opinion, based on information or material in his possession, that the provisions of any other law for the time being in force are contravened, then the Director or such other authority shall share the information with the concerned agency for necessary action.

## Summary

The Benami Transaction (Prohibition) Act is "an Act to prohibit benami transactions and the right to recover property held benami for matters connected therewith or incidental thereto."

Benami Transaction, transaction or arrangement, where consideration is provided by a person other than the transferee or the person, in whose name property is held. Exceptions; the following transaction would not be regarded as "benami transactions;

- Karta or member of HUF holding HUF property if consideration for the property provided or paid out of known sources of HUF;
- Property held by a person standing in a fiduciary capacity;
- Property held in the name of spouse or any child of an individual and consideration for property paid or provided out of known sources of individual;
- Property held jointly in the names of an individual and his brother/sister/lineal ascendant/ lineal descendant, where consideration for property paid or provided out of known sources of individual;
- Genuine stamp duty paid Power of Attorney transactions referred to in Section 53A of the Transfer of Property Act, where the contract (agreement to sell) is registered and the transferee has taken possession and paid consideration to the transferor but the property remains in transferors' name.

The Money Laundering Act is "an Act to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money laundering and for matters connected therewith or incidental thereto".

Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to a fine.

## Keywords

Benami property: It means any property which is the subject matter of a benami transaction and also includes the proceeds from such property.

Benami transaction: It means a transaction or an arrangement where a property is transferred to, or is held by, a person, and the consideration for such property has been provided, or paid by, another person

Benamidar: This term means a person or a fictitious person, as the case may be, in whose name the benami property is transferred or held and includes a person who lends his name.

Beneficial owner: It means a person, whether his identity is known or not, for whose benefit the benami property is held by a benamidar.

Coparcener: He or She is a person who shares equally with others in the inheritance of an undivided estate or in the rights to it.

Financial institution: It means a financial institution as defined in clause (c) of section 45-1 of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company, a housing finance institution, an authorized person, a payment system operator, a non-banking financial company and the Department of Posts in the Government of India.

Initiating Officer: It means an Assistant Commissioner or a Deputy Commissioner as defined in clauses (9A) and (19A) respectively of section 2 of the Income-tax Act, 1961 (43 of 1961).

Money laundering: It involves disguising one's financial assets, so that they can be used without detection of the illegal activity that led to its production. Through the process of money laundering, a person converts illegal money into a legal entity.

Property: It means assets of any kind, whether movable or immovable, tangible or intangible, corporeal or incorporeal and includes any right or interest or legal documents or instruments evidencing title to or interest in the property and where the property is capable of conversion into some other form, then the property in the converted form and also includes the proceeds from the property.

Transfer: It includes sale, purchase or any other form of transfer of right, title, possession or lien.

Value: It means the fair market value of any property on the date of its acquisition by any person, or if such date cannot be determined, the date on which such property is possessed by such person.

## SelfAssessment

1. A transaction or an arrangement whereby a property is transferred to a person and the consideration for such property has been paid by another person is an example of:

A. A business transaction
B. A Benami transaction
C. A barter transaction
D. A personal transaction

2. Which of the following is an exception to benami transaction?

A. Property is held for the benefit of Karta and the consideration for such property has been paid out of the known sources of the Hindu undivided family.
B. a transaction or an arrangement in respect of a property where the person providing the consideration is not traceable or is fictitious.
C. a transaction or an arrangement in respect of a property carried out or made in a fictitious name.

D. a transaction or an arrangement in respect of a property where the owner of the property is not aware of, or, denies knowledge of, such ownership.

3. If any person enters into any benami transaction, he/she shall be liable of:
A. Imprisonment for a term that may extend to three years
B. Imprisonment for a term that may extend to ten years
C. Imprisonment for a term that may extend to three years or/and a Fine
D. Imprisonment for a term that may extend to ten years or/and a Fine

4. Any property, which is a subject matter of benami transaction, shall be liable to be confiscated by the _____.
A. Adjudicating Authority
B. State Government
C. Central Government
D. Income Tax Department

5. Which of the following is not considered the Powers of authorities under the Benami Transaction (Prohibition) Act, 1988?
A. compelling the production of books of account and other documents
B. discovery and inspection
C. issuing evidence on affidavits
D. issuing commissions

6. The Central Government shall, by notification, establish _____ to hear appeals against the orders of any authority under this Act.
A. an Appellate Tribunal
B. an Adjudicating Authority
C. a bench of officers
D. a bench of initiating officers

7. Where any person enters into a benami transaction to defeat the provisions of any law and is found guilty of the offence of benami transaction, he/she shall be liable for:
A. imprisonment of at least 1 year
B. imprisonment of 7 years
C. fine which may extend to twenty-five per cent of the fair market value of the property
D. imprisonment for a term of 1-7 years and a fine which may extend to twenty-five per cent of the fair market value of the property

8. Any person who is required to furnish information under the Benami Transaction (Prohibition) Act, 1988 knowingly gives false information to any authority under this Act, shall be punishable with:
A. Maximum 6 months imprisonment
B. Maximum 5 months imprisonment
C. Maximum 3 years imprisonment
D. Maximum 5 years imprisonment

9. Section 3 of the Money Laundering Act, 2002 deals with:

A. Offence of money-laundering
B. Punishment for money-laundering
C. Reporting entity to maintain records
D. Access to information

10. Whoever commits the offence of money-laundering shall be punishable with:
A. imprisonment of less than 3 years
B. imprisonment of not less than 3 years
C. imprisonment of not less than 3 years but which may extend to seven years
D. imprisonment of not less than 3 years but which may extend to seven years and shall also be liable to fine

11. When a Director can initiate an inquiry under the Money Laundering Act, 2002?
A. By his motion, if he thinks fit to be necessary, concerning the obligations of the reporting entity
B. On an application made by any authority, officer or person, if he thinks fit to be necessary, concerning the obligations of the reporting entity
C. By his motion or on an application made by any authority, officer or person, if he thinks fit to be necessary, concerning the obligations of the reporting entity
D. No restriction, a Director can anytime initiate any inquiry

12. Any reporting entity which is aggrieved by any order of the Director can file an appeal against the order to:
A. High Court
B. Appellate Tribunal
C. State Government
D. Central Government

13. An appeal against the order of Adjudicating Authority has to be filed within _____ from the date on which a copy of the order made by the Adjudicating Authority or Director is received.
A. 30 days
B. 45 days
C. 60 days
D. 15 days

14. Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the _____
A. High Court
B. Supreme Court
C. State Government
D. Central Government

15. The High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the sixty days, allow it to be filed within a further period not exceeding_____.
A. 30 days

B. 45 days
C. 60 days
D. 90 days

## Answers for Self Assessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | B | 2. | A | 3. | C | 4. | C | 5. | C |
| 6. | A | 7. | D | 8. | D | 9. | A | 10. | D |
| 11. | C | 12. | B | 13. | B | 14. | A | 15. | C |

## Review Questions

1. Explain Benami Transactions.
2. Explain the provisions of the following Sections of the Benami Transaction (Prohibition) Act, 1988:
   a. Section 3
   b. Section 4
   c. Section 6
   d. Section 18
   e. Section 19
3. List the Authorities and their Jurisdiction that can be established under the Benami Transaction (Prohibition) Act, 1988. Explain the powers of the Authorities as well.
4. Is there any prohibition on re-transfer of property by Benamidar? Justify.
5. Is there any prohibition of the right to recover property held benami? Justify.
6. If adjudicating authority under the Benami Transaction (Prohibition) Act, 1988 is working on a certain case and required to undertake a detailed inquiry, then is it required for it to work on its own or it can be assisted by other officers? Explain.
7. Discuss the penalty for benami transactions and false information.
8. When a person is found guilty of the offence of money-laundering and what is the punishment for the same under the Money Laundering Act, 2002?
9. Discuss the provisions of Section 12 related to reporting entity to maintain records.
10. Explain the powers of a Director to impose a fine under the Money Laundering Act, 2002.
11. Explain the provisions related to "Search and Seizure" under the Money Laundering Act, 2002.
12. Explain the redressal body and redressal mechanism under the Money Laundering Act, 2002.

## Further Readings

Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.

### Web Links

https://www.indiacode.nic.in/handle/123456789/1840?sam_handle=123456789/1362

https://www.mondaq.com/india/white-collar-crime-anti-corruption--fraud/678174/understanding-the-benami-law-in-india-frequently-asked-questions

https://incometaxindia.gov.in/Booklets%20%20Pamphlets/13-keep-away-from-benami-transaction.pdf

https://www.indiacode.nic.in/handle/123456789/2036?sam_handle=123456789/1362#:~:text=India%20Code%3A%20Prevention%20of%20Money%2DLaundering%20Act%2C%202002&text=Go!&text=Long%20Title%3A,connected%20therewith%20or%20incidental%20thereto.

https://taxguru.in/income-tax/benami-transactions-benami-property.html

# Unit 12: Regulatory Measures for Curbing Corporate Fraud-3

CONTENTS



## Objectives

After studying this unit, you will be able to:

- summarize the relevant provisions of the Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003 to curb and prevent Corporate Fraud.
- summarize the relevant provisions of the Indian Penal Code (1860) to curb or prevent Corporate Fraud.

## Introduction

The Securities market is a part of the financial market where buying and selling of securities are done. Just like any other financial market, securities market is also prone to scams, frauds and illicit activities. Securities market in India involves millions of active investors on a daily basis investing and earning money through the trade done. So it is very essential to check and prevent any of the scams or frauds in the market to safeguard the interests of all the investors in the securities market.

The Prohibition of fraudulent and unfair trade practices regulation passed on July 17, 2003 lists down the various points as unacceptable in securities market for regulating the securities market from frauds and scams. Chapter II (3) of this regulation deals with prohibition of unfair dealings in securities.

Securities and Exchange Board of India (SEBI) plays a pivotal and instrumental role in prohibiting any sort of activities that are manipulative or fraudulent or unfair in the securities market. After SEBI encountered many unfair practices, frauds that affect the securities market, SEBI passed a special regulation pertaining to prohibition of manipulative, fraudulent and unfair trade practices in chapter II (4) of 2003 regulation. These regulations are discussed in this unit along some relevant sections of the Indian Penal Code, 1860 for preventing and curbing Corporate and individual scams.

## 12.1 Provisions of Unfair Trade Practices Relating to Security Market

Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003

(1) These regulations may be called the Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

These regulations are read with Securities Exchange Board of India Act, 1992, formed by SEBI Board for prohibition of fraudulent, manipulative and unfair trade practices relating to the Securities Market, with an object to prohibit; buy, sell or otherwise deal in securities in the fraudulent manner; use or employ of any manipulative or deceptive device in contravention of provisions of SEBI Act; and to engage in any act, practice of fraud in connection with dealing or issue of securities.

### Regulation 2 (Chapter I)

2. (1) In these regulations, unless the context otherwise requires, —

(a) "Act" means the Securities and Exchange Board of India Act, 1992 (15 of 1992);

(b) "dealing in securities" includes:

(i) an act of buying, selling or subscribing pursuant to any issue of any security or agreeing to buy, sell or subscribe to any issue of any security or otherwise transacting in any way in any security by any persons including as principal, agent, or intermediary referred to in section 12 of the Act;

(ii) such acts which may be knowingly designed to influence the decision of investors in securities; and

(iii) any act of providing assistance to carry out the aforementioned acts.

"fraud" includes any act, expression, omission or concealment committed whether in a deceitful manner or not by a person or by any other person with his connivance or by his agent while dealing insecurities in order to induce another person or his agent to deal in securities, whether or not there is any wrongful gain or avoidance of any loss, and shall also include-

(1) a knowing misrepresentation of the truth or concealment of material fact in order that another person may act to his detriment;

(2) a suggestion as to a fact which is not true by one who does not believe it to be true;

(3) an active concealment of a fact by a person having knowledge or belief of the fact;

(4) a promise made without any intention of performing it;

(5) a representation made in a reckless and careless manner whether it be true or false;

(6) any such act or omission as any other law specifically declares to be fraudulent,

(7) deceptive behavior by a person depriving another of informed consent or full participation,

(8) a false statement made without reasonable ground for believing it to be true.

(9) The act of an issuer of securities giving out misinformation that affects the market price of the security, resulting in investors being effectively misled even though they did not rely on the statement itself or anything derived from it other than the market price.

And "fraudulent" shall be construed accordingly;

Nothing contained in this clause shall apply to any general comments made in good faith in regard to—

(a) the economic policy of the government

(b) the economic situation of the country

(c) trends in the securities market or

(d) any other matter of a like nature

whether such comments are made in public or in private;

(d) "Investigating Authority" means any person authorized by the Board to undertake investigation under section11C of the Act;

(e) "securities" means securities as defined in section 2 of the Securities Contracts(Regulation) Act, 1956 (42 of 1956).

### Regulation 3 (Chapter II): Prohibition of fraudulent and unfair trade practices relating to the securities market

3. Prohibition of certain dealings in securities

No person shall directly or indirectly ─

(a) buy, sell or otherwise deal in securities in a fraudulent manner;

(b) use or employ, in connection with issue, purchase or sale of any security listed or proposed to be listed in a recognized stock exchange, any manipulative or deceptive device or contrivance in contravention of the provisions of the Act or the rules or the regulations made there under;

(c) employ any device, scheme or artifice to defraud in connection with dealing in or issue of securities which are listed or proposed to be listed on a recognized stock exchange;

(d) engage in any act, practice, course of business which operates or would operate as fraud or deceit upon any person in connection with any dealing in or issue of securities which are listed or proposed to be listed on are cognized stock exchange in contravention of the provisions of the Act or the rules and the regulations made there under.

### Regulation 4 (Chapter II): Prohibition of manipulative, fraudulent and unfair trade practices

(1) Without prejudice to the provisions of regulation, no person shall indulge in a manipulative, fraudulent or an unfair trade practice in securities markets;

(2) Dealing in securities shall be deemed to be a manipulative fraudulent or an unfair trade practice if it involves any of the following: ─

(a) knowingly indulging in an act which creates false or misleading appearance of trading in the securities market;

(b) Dealing in a security not intended to effect transfer of beneficial ownership but intended to operate only as a device to inflate, depress or cause fluctuations in the price of such security for wrongful gain or avoidance of loss;

(c) inducing any person to subscribe to an issue of the securities for fraudulently securing the minimum subscription to such issue of securities, by advancing or agreeing to advance any money to any other person or through any other means;

(d) inducing any person for dealing in any securities for artificially inflating, depressing, maintaining or causing fluctuation in the price of securities through any means including by paying, offering or agreeing to pay or offer any money or money's worth, directly or indirectly, to any person;

(e) any act or omission amounting to manipulation of the price of a security including, influencingor manipulating the reference price or bench mark price of any securities;

(f) knowingly publishing or causing to publish or reporting or causing to report by a person dealing in securities any information relating to securities, including financial results, financial statements, mergers and acquisitions, regulatory approvals, which is not true or which he does not believe to be true prior to or in the course of dealing in securities;

(g) Entering into a transaction in securities without intention of performing it or without intention of change of ownership of such security;

(h) selling, dealing or pledging of stolen, counterfeit or fraudulently issued securities whether in physical or dematerialized form:

Provided that if: -

(i) the person selling, dealing in or pledging stolen, counterfeit or fraudulently issued securities was a holder in due course; or

(ii) the stolen, counterfeit or fraudulently issued securities were previously traded on the market through a bonafide transaction,

(iii) such selling, dealing or pledging of stolen, counterfeit or fraudulently issued securities shall not be considered as a manipulative, fraudulent, or unfair trade practice;

Caution: I, j clauses are omitted

(k) disseminating information or advice through any media, whether physical ordigital, which the disseminator knows to be false or misleading in a reckless orcareless manner and which is designed to, or likely to influence the decision of investors dealing in securities;

Caution: L clause is omitted

(m) a market participant entering into transactions on behalf of client without the knowledge of or instructions from client or mis-utilizing or diverting the funds or securities of the client held in fiduciary capacity

(n) circular transactions in respect of a security entered into between persons includingintermediaries to artificially provide a false appearance of trading in such security or to inflate, depress or cause fluctuations in the price of such security;

(o) fraudulent inducement of any person by a market participant to deal in securities with the objective of enhancing his brokerage or commission or income;

(p) an intermediary predating or otherwise falsifying records including contract notes, client instructions, balance of securities statement, client account statements

(q) any order in securities placed by a person, whiledirectly or indirectly inpossession of information that is not publically available, regarding a substantial impending transaction in that securities, its underlying securities or its derivative;

(r) knowingly planting false or misleading news which may induce sale or purchase of securities.

(s) mis-selling of securities or services relating to securities market;

For the purpose of this clause, "mis-selling" means sale of securities or services relating to securities market by any person, directly or indirectly, by—

(i) knowingly making a false or misleading statement, or

(ii) knowingly concealing or omitting material facts, or

(iii) knowingly concealing the associated risk, or

iv) not taking reasonable care to ensure suitability of the securities or service to the buyer

(t) illegal mobilization of funds by sponsoring or causing to be sponsored or carrying on or causing to be carried on any collective investment scheme by any person.

## 12.2 Provisions of the Indian Penal Code, 1860

**Section 2. Punishment of offences committed within India.**

Every person shall be liable to punishment under this Code and not otherwise for every act or omission contrary to the provisions thereof, of which he shall be guilty within India.

**Section 3. Punishment of offences committed beyond, but which by law may be tried within, India.**

Any person liable, by any Indian law, to be tried for an offence committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act had been committed within India.

**Section 4. Extension of Code to extra-territorial offences.**

-- The provisions of this Code apply also to any offence committed by

(1) any citizen of India in any place without and beyond India;

(2) any person on any ship or aircraft registered in India wherever it may be.

(3) any person in any place without and beyond India committing offence targeting a computer resource located in India.

A, who is a citizen of India, commits a murder in Uganda. He can be tried and convicted of murder in any place in India in which he may be found.

**Task:**

1. Define person as per the Indian Penal Code, 1860. [Hint: Refer Sec. 11]

2. What does "Court of Justice" denote as per the Indian Penal Code, 1860. [Hint: Refer Sec. 20]

### Section 23. "Wrongful gain".

"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

"Wrongful loss". —"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

Gaining wrongfully/Losing wrongfully. —A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

### Section 53. Punishments.

The punishments to which offenders are liable under the provisions of this Code are —

First—Death;

Secondly—Imprisonment for life;

Caution: Thirdly is Omitted

Fourthly—Imprisonment, which is of two descriptions, namely: —

(1) Rigorous, that is, with hard labor;

(2) Simple;

Fifthly—Forfeiture of property;

Sixthly—Fine

### Section 120A. Definition of criminal conspiracy.

When two or more persons agree to do, or cause to be done,

(1) an illegal act, or

(2) an act which is not illegal by illegal means, such an agreement is designated a criminal conspiracy:

Provided that no agreement except an agreement to commit an offence shall amount to a criminal conspiracy unless some act besides the agreement is done by one or more parties to such agreement in pursuance thereof.

Explanation. It is immaterial whether the illegal act is the ultimate object of such agreement, or is merely incidental to that object.

### Section 120B. Punishment of criminal conspiracy.

(1) Whoever is a party to a criminal conspiracy to commit an offence punishable with death, imprisonment for life or rigorous imprisonment for a term of two years or upwards, shall, where no express provision is made in this Code for the punishment of such a conspiracy, be punished in the same manner as if he had abetted such offence.

(2) Whoever is a party to a criminal conspiracy other than a criminal conspiracy to commit an offence punishable as aforesaid shall be punished with imprisonment of either description for a term not exceeding six months, or with fine or with both.

### Section 264. Fraudulent use of false instrument for weighing.

Whoever, fraudulently uses any instrument for weighing which he knows to be false, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

**Section 403. Dishonest misappropriation of property.**

Whoever dishonestly misappropriates or converts to his own use any movable property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

A takes property belonging to Z out of Z's possession, in good faith believing at the time when he takes it, that the property belongs to himself. A is not guilty of theft; but if A, after discovering his mistake, dishonestly appropriates the property to his own use, he is guilty of an offence under this section.

**Section 405. Criminal breach of trust.**

Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits "criminal breach of trust".

A, being executor to the will of a deceased person, dishonestly disobeys the law which directs him to divide the effects according to the will, and appropriates them to his own use. A has committed criminal breach of trust.

**Section 406. Punishment for criminal breach of trust.**

Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

**Section 407. Criminal breach of trust by carrier, etc.**

Whoever, being entrusted with property as a carrier, wharfinger or warehouse-keeper, commits criminal breach of trust in respect of such property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

**Section 409. Criminal breach of trust by public servant or by banker, merchant or agent.**

Whoever, being in any manner entrusted with property, or with any dominion over property in his capacity of a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

**Section 410. Stolen property.**

Property, the possession whereof has been transferred by theft, or by extortion, or by robbery, and property which has been criminally misappropriated or in respect of which criminal breach of trust has been committed, is designated as "stolen property", whether the transfer has been made, or the misappropriation or breach of trust has been committed, within or without India. But, if such property subsequently comes into the possession of a person legally entitled to the possession thereof, it then ceases to be stolen property.

**Section 411. Dishonestly receiving stolen property.**

Whoever dishonestly receives or retains any stolen property, knowing or having reason to believe the same to be stolen property, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

**Section 415. Cheating.**

Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation. —A dishonest concealment of facts is a deception within the meaning of this section.

(a) A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

(b) A, by putting a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.

© A, by exhibiting to Z a false sample of an article intentionally deceives Z into believing that the article corresponds with the sample, and thereby dishonestly induces Z to buy and pay for the article. A cheats.

### Section 417. Punishment for cheating.

Whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

### Section 416. Cheating by personation.

A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for or another, or representing that he or any other person is a person other than he or such other person really is.

Explanation. —The offence is committed whether the individual personated is a real or imaginary person.

(a) A cheats by pretending to be a certain rich banker of the same name. A cheats by by personation.

(b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

### Section 419. Punishment for cheating by personation.

Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

### Section 418. Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect.

Whoever cheats with the knowledge that he is likely thereby to cause wrongful loss to a person whose interest in the transaction to which the cheating relates, he was bound, either by law, or by a legal contract, to protect, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

### Section 420. Cheating and dishonestly inducing delivery of property.

Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

### Section 421. Dishonest or fraudulent removal or concealment of property to prevent distribution among creditor.

Whoever dishonestly or fraudulently removes, conceals or delivers to any person, or transfers or causes to be transferred to any person, without adequate consideration, any property, intending thereby to prevent, or knowing it to be likely that he will thereby prevent, the distribution of that property according to law among his creditors or the creditors of any other person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

### Section 463. Forgery.

Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

### Section 464. Making a false document.

A person is said to make a false document or false electronic record—

First. —Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any electronic signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the electronic signature,

with the intention of causing it to be believed that such document or part of document, electronic record or electronic signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, singed, sealed, executed or affixed; or

Secondly. —Who without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with electronic signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly. —Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his electronic signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alteration.

### Section 465. Punishment for forgery.

Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

### Section 468. Forgery for purpose of cheating.

Whoever commits forgery, intending that the document or electronic record forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

### Section 469. Forgery for purpose of harming reputation.

Whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

### Section 470. Forged document.

A false document or electronic record made wholly or in part by forgery is designated "a forged document or electronic record".

### Section 471. Using as genuine a forged document or electronic record.

Whoever fraudulently or dishonestly uses as genuine any document or electronic record which he knows or has reason to believe to be a forged document or electronic record, shall be punished in the same manner as if he had forged such document or electronic record.

### Section 472. Making or possessing counterfeit seal, etc., with intent to commit forgery punishable under section 467.

Whoever makes or counterfeits any seal, plate or other instrument for making an impression, intending that the same shall be used for the purpose of committing any forgery which would be punishable under section 467 of this Code, or, with such intent, has in his possession any such seal, plate or other instrument, knowing the same to be counterfeit, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

**Section 477. Fraudulent cancellation, destruction, etc., of will, authority to adopt, or valuable security.**

Whoever fraudulently or dishonestly, or with intent to cause damage or injury to the public or to any person, cancels, destroys or defaces, or attempts to cancel, destroy or deface, or secretes or attempts to secrete any document which is or purports to be a will, or an authority to adopt a son, or any valuable security, or commits mischief in respect of such document, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

**Section 477A. Falsification of accounts.**

Whoever, being a clerk, officer or servant, or employed or acting in the capacity of a clerk, officer or servant, wilfully, and with intent to defraud, destroys, alters, mutilates or falsifies any 2[book, electronic record, paper, writing] valuable security or account which belongs to or is in the possession of his employer, or has been received by him for or on behalf of his employer, or wilfully, and with intent to defraud, makes or abets the making of any false entry in, or omits or alters or abets the omission or alteration of any material particular from or in. any such 2[book, electronic record, paper, writing] valuable security or account, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

**Section 481. Using a false property mark.**

Whoever marks any movable property or goods or any case, package or other receptacle containing movable property or goods, or uses any case, package or other receptacle having any mark thereon, in a manner reasonably calculated to cause it to be believed that the property or goods so marked, or any property or goods contained in any such receptacle so marked, belong to a person to whom they do not belong, is said to use a false property mark.

**Section 482. Punishment for using a false property mark.**

Whoever uses any false property mark shall, unless he proves that he acted without intent to defraud, be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

**Section 483. Counterfeiting a property mark used by another.**

Whoever counterfeits any property mark used by any other person shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

**Section 486. Selling goods marked with a counterfeit property mark.**

Whoever sells, or exposes, or has in possession for sale, any goods or things with a counterfeit property mark affixed to or impressed upon the same or to or upon any case, package or other receptacle in which such goods are contained, shall, unless he proves

(a) that, having taken all reasonable precautions against committing an offence against this section, he had at the time of the commission of the alleged offence no reason to suspect the genuineness of the mark, and

(b) that, on demand made by or on behalf of the prosecutor, he gave all the information in his power with respect to the persons from whom he obtained such goods or things, or

(c) that otherwise he had acted innocently, be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

**Section 487. Making a false mark upon any receptacle containing goods.**

Whoever makes any false mark upon any case, package or other receptacle containing goods, in a manner reasonably calculated to cause any public servant or any other person to believe that such receptacle contains goods which it does not contain or that it does not contain goods which it does contain, or that the goods contained in such receptacle are of a nature or quality different from the real nature or quality thereof, shall, unless he proves that he acted without intent to defraud, be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

**Section 488. Punishment for making use of any such false mark.**

Whoever makes use of any such false mark in any manner prohibited by the last foregoing section shall, unless he proves that he acted without intent to defraud, be punished as if he had committed an offence against that section.

**Section 489. Tampering with property mark with intent to cause injury.**

Whoever removes, destroys, defaces or adds to any property mark, intending or knowing it to be likely that he may thereby cause injury to any person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

**Task:**Discuss the provisions related to Defamation as per the Indian Penal Code, 1860.

[Hint Refer Sec. 499]

**Section 511. Punishment for attempting to commit offences punishable with imprisonment for life or other imprisonment.**

Whoever attempts to commit an offence punishable by this Code with imprisonment for life or imprisonment, or to cause such an offence to be committed, and in such attempt does any act towards the commission of the offence, shall, where no express provision is made by this Code for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the imprisonment for life or, as the case may be, one- half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

Illustrations

(a) A makes an attempt to steal some jewels by breaking open a box, and finds after so opening the box, that there is no jewel in it. He has done an act towards the commission of theft, and therefore is guilty under this section.

(b) A makes an attempt to pick the pocket of Z by thrusting his hand into Z's pocket. A fails in the attempt in consequence of Z's having nothing in his pocket. A is guilty under this section

## Summary

Securities and Exchange Board of India (SEBI) plays a pivotal and instrumental role in prohibiting any sort of activities that are manipulative or fraudulent or unfair in the securities market. After SEBI encountered many unfair practices, frauds that affect the securities market, SEBI passed a special regulation pertaining to prohibition of manipulative, fraudulent and unfair trade practices in chapter II (4) of 2003 regulation.

For any market to flourish and maintain a constant growth on a long-term, it is necessary to maintain the market free from any frauds, illicit activities, unfair and manipulative actions. This goes same with Securities market. In order to maintain a long-term growth and protect the people involved in investing in the securities market, the Securities and Exchange Board of India (SEBI) has taken every step possible to maintain the same with all possible means. In India owing to population and many investors entering into the market, there is a greater risk for any frauds to occur capitalizing from a large number of investors and also in the modern technological era, India lags behind cybersecurity compared to other developed countries. Since most securities are handled now through online platforms, applications etc. SEBI should also bring in the cybersecurity guidelines and cyber security wing to protect the securities market from any possible cyber hacking eventually protecting and guiding securities market in India to a path of development.

The Indian Penal Code is the official criminal code of the Republic of India. It is a complete code intended to cover all aspects of criminal law. The IPC in its various sections defines specific crimes and provides punishment for them. It is sub-divided into 23 chapters that comprise of 511 sections.

## Keywords

Act: The word "act" denotes as well as series of acts as a single act.

Counterfeit: A person is said to "counterfeit" who causes one thing to resemble another thing, intending by means of that resemblance to practice deception, or knowing it to be likely that deception will thereby be practiced.

Defamation: Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

Dishonestly: Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Fraudulently: A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Illegal: The word "illegal" is applicable to everything which is an offence or which is prohibited by law, or which furnishes ground for a civil action.

Legally bound to do: A person is said to be "legally bound to do" whatever it is illegal in him to omit.

Omission: The word "omission" denotes as well a series of omissions as a single omission.

## SelfAssessment

1. Prohibition of unfair dealings in securities regulation states that:

A. No one should employ any scheme or device or strategy to defraud the dealings connected with securities.
B. No person shall indulge in fraud or unfair trade practices in the securities market.
C. Creating a fake appearance of trading securities that would give a false appearance of trading to investors is not allowed.
D. Handling securities to inflate or cause fluctuations in securities is not allowed instead it should be intended for transfer of ownership only.

2. Prohibition of unfair dealings in securities regulation does not state that:

A. Nobody directly or indirectly should indulge in fraud relating to selling, buying or dealing with securities;
B. No one should use any manipulative or deceptive means to violate the provisions of the Act;
C. No one should employ any scheme or device or strategy to defraud the dealings connected with securities.
D. Any act to manipulate the price of securities is not allowed.

3. Prohibition of Manipulative, Fraudulent and Unfair trade practices regulation states that:

A. Nobody directly or indirectly should indulge in fraud relating to selling, buying or dealing with securities
B. No one should use any manipulative or deceptive means to violate the provisions of the Act
C. Use of any information that is false to make a person handle with securities is not allowed.
D. No one should employ any scheme or device or strategy to defraud the dealings connected with securities.

4. Prohibition of Manipulative, Fraudulent and Unfair trade practices regulation does not state that:

A. Handling securities to inflate or cause fluctuations in securities is not allowed instead it should be intended for transfer of ownership only.
B. To pay any person money or money's equivalent to handle securities with the motive of causing fluctuations or inflation is not allowed.
C. To handle securities with any intention of performing or with the intention of change in ownership is not allowed.
D. Should not deal with any securities that are stolen or fake.

5. Regulations related to the Prohibition of Manipulative, Fraudulent and Unfair trade practices are given in the following Regulation of Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market) Regulations, 2003:

A. Regulation 3 of Chapter I
B. Regulation 3 of Chapter II
C. Regulation 4 of Chapter I
D. Regulation 4 of Chapter II

6. The punishments to which offenders are liable under the provisions of the Indian Penal Code, 1869 include:

A. Death
B. Imprisonment for life
C. Forfeiture of property
D. All

7. Amit attempts to pick the pocket of Ashwin by thrusting his hand into Ashwin's pocket. Amit fails in the attempt in consequence of Ashwin's having nothing in his pocket. Amit is guilty under which section the Indian Penal Code, 1860

A. Section 465
B. Section 488
C. Section 489
D. Section 511

8. Whoever commits forgery shall be punished:

A. with imprisonment of either description for a term which may extend to two years
B. with fine
C. with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
D. With life time imprisonment and fine

9. Any person who is found guilty of selling goods marked with a counterfeit property mark shall be punished with:

A. imprisonment of either description for a term which may extend to one year, or with fine, or with both.
B. imprisonment of either description for a term which may extend to two years, or with fine, or with both.

C. imprisonment of either description for a term which may extend to three years, or with fine, or with both.
D. imprisonment of either description for a term which may extend to five years, or with fine, or with both.

10. Whoever cheats by personation shall be punished with:
A. imprisonment of either description for a term which may extend to two years, or with fine, or with both.
B. imprisonment of either description for a term which may extend to three years, or with fine, or with both.
C. imprisonment of either description for a term which may extend to five years, or with fine, or with both.
D. imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

11. Section 417 of the Indian Penal Code, 1860 deals with:
A. Punishment for Forgery
B. Punishment for False statement
C. Punishment for Cheating
D. Punishment for Cheating by personation

12. Whoever commits criminal breach of trust shall be punished with:
A. imprisonment of either description for a term which may extend to one year, or with fine, or with both.
B. imprisonment of either description for a term which may extend to two years, or with fine, or with both.
C. imprisonment of either description for a term which may extend to three years, or with fine, or with both.
D. imprisonment of either description for a term which may extend to four years, or with fine, or with both.

13. Section 120B of the Indian Penal Code, 1860 deals with:
A. Definition of criminal conspiracy
B. Punishment of criminal conspiracy
C. Fraudulent use of false instrument
D. Fraudulent use of false instrument for weighing

14. Section 411 of the Indian Penal Code, 1860 deals with:
A. Criminal breach of trust by the public servant
B. Stolen property
C. Dishonestly receiving stolen property
D. Cheating

15. Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person shall be punished with:

A. imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.
B. imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.
C. imprisonment of either description for a term which may extend to six years, and shall also be liable to fine.
D. imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

## Answers forSelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | A | 2. | D | 3. | C | 4. | C | 5. | D |
| 6. | D | 7. | D | 8. | C | 9. | A | 10. | B |
| 11. | C | 12. | C | 13. | B | 14. | C | 15. | D |

## Review Questions

1. Discuss Regulation 2 of Prohibition of Fraudulent and Unfair Trade Practices relating to the Securities Market) Regulations, 2003.
2. Discuss Regulation 3 related to the Prohibition of fraudulent and unfair trade practices relating to the securities market.
3. Discuss Regulation 4 related to the Prohibition of manipulative, fraudulent and unfair trade practices.
4. Discuss the following sections of the Indian Penal Code, 1860:
   a. Section 53
   b. Section 120 A
   c. Section 120 B
   d. Section 405 along with the provisions of Section 406
   e. Section 410
5. Discuss the punishments for the following as per the provisions of the Indian Penal Code, 1860:
   a. Dishonestly receiving stolen property
   b. Cheating
   c. Forgery
   d. Using false property mark
   e. Criminal breach of trust
6. Discuss various sections along with their provisions related to false property marks and counterfeit property marks.
7. Discuss punishment for attempting to commit offences punishable with imprisonment for life or other imprisonments.
8. What is criminal conspiracy? Which punishments are prescribed for criminal conspiracy in the Indian Penal Code, 1860?

## Further Readings


- Gupta, D. S. (2016). *Corporate Frauds & their Regulation in India* (First ed.). Bharat Law House PVT. LTD.


### Web Links

- https://www.sebi.gov.in/legal/regulations/jan-2022/securities-and-exchange-board-of-india-prohibition-of-fraudulent-and-unfair-trade-practices-relating-to-securities-market-regulations-2003-last-amended-on-january-25-2022-_55604.html
- https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362
- https://blog.ipleaders.in/fraudulent-and-unfair-trade-practices/

# Unit 13: Digital Forensics and Cyber Laws

CONTENTS



## Objectives

After studying this unit, you will be able to:

- explain the meaning, types and sources of digital data.
- illustrate the process of digital forensics.
- evaluate the role of blockchain technology in digital forensics.
- evaluate the objectives of National Cyber Security Policy, 2013.
- explain relevant Cyber laws and regulations.

## Introduction

Digital forensics is the process of uncovering and analyzing digital evidence in order to investigate and solve crimes, as well as to prevent future incidents. There are several reasons why digital forensics is important:

**Investigating cybercrimes**: With the increasing use of technology, criminals are now using digital means to commit crimes such as fraud, hacking, identity theft, and other cybercrimes. Digital forensics plays a crucial role in uncovering evidence of such crimes and identifying the culprits.

**Preventing insider threats:**Digital forensics can help identify and prevent insider threats by monitoring and analyzing employee behavior and activities. This can help detect and prevent data breaches, theft, and other security incidents.

**Supporting legal cases:**Digital evidence is increasingly being used in legal cases, and digital forensics is used to collect and analyze this evidence to support court proceedings. This can include email communications, social media posts, and other digital data.

**Protecting intellectual property:**Digital forensics can be used to identify and prevent intellectual property theft, such as stealing trade secrets, patents, and copyrights.

**Responding to incidents**: Digital forensics can help organizations respond to security incidents, such as data breaches, by analyzing and identifying the cause of the incident, the extent of the damage, and the steps needed to prevent future incidents.

Thus, at a time when everything has become digital, from banking, offices, and shopping, to education. The National Cyber Security has become more critical for security on Digital Platform. Stringent Cyber Security policy is the need of the hour as India has risen among the Cyber-Attacked countries. Post pandemic lockdown Cyber Crimes have increased tremendously. It poses a threat not only to citizens and businesses but also to our Defense forces and government. Over the years' digitalization has tossed convenience and quicker solutions but it has grown more complex and vulnerable.In the present unit, types of digital data and digital forensics are discussed along with cyber laws applicable in India.

## 13.1 Overview of Digital Data

Digital data refers to information that is stored in electronic form and can be processed by computers. This data can come in various formats, such as text, images, audio, video, and other forms. The rise of digital technology has led to an explosion in the amount of data being generated, with estimates suggesting that the total amount of data created in the world is doubling every two years.

## 13.2 Sources and Types of Digital Data

### Sources of Digital Data

Digital data can be generated from various sources, including:

1. Electronic devices: Digital data can be generated from electronic devices such as computers, smartphones, smart TVs and tablets, as well as wearable devices like smartwatches and fitness trackers.

2. Social media: Social media platforms such as Facebook, Twitter, Instagram, and LinkedIn generate vast amounts of digital data in the form of user-generated content, interactions, and behavior.

3. E-commerce: Online shopping and e-commerce generate digital data in the form of purchase history, search queries, and user behavior.

4. Internet of Things (IoT): The Internet of Things refers to the network of devices and sensors that are connected to the internet, generating large amounts of data in real-time.

### Types of Digital Data

Digital data can be classified into several types, including:

1. Structured data: Structured data refers to data that is organized in a specific format, such as tables, spreadsheets, and databases. This type of data is easy to search and analyze using computer programs.

Examples

Relational databases, Spreadsheets, XML and JSON files, CSV files, Log files, Sensor data, Financial data, Medical records

2. Unstructured data: Unstructured data refers to data that does not have a specific format, such as text documents, images, and videos. This type of data is more difficult to search and analyze using traditional computer programs.

Examples

Text data (emails; social media posts; chat messages; news articles etc.), Multimedia data (Digital images; Videos; Audio recording etc.), Web pages, Social media data, Email attachments, Voice recordings.

3. Semi-structured data: Semi-structured data refers to data that has some structure, but is not fully organized. Examples include email messages, XML files, and JSON data.

4. Big data: Big data refers to extremely large data sets that cannot be easily processed or analyzed using traditional methods. Big data typically involves a mix of structured, unstructured, and semi-structured data.

5. Analog Data: Analog data is continuous data that varies in a smooth manner over time. This type of data is represented by a continuous signal that can take on an infinite number of values within a specific range. For example, sound waves, temperature, and pressure are examples of analog data.

6. Digital Data: Digital data is a discrete data that is represented by a series of binary digits (0s and 1s). This type of data is processed and stored in a digital format, making it easier to manipulate and transmit. Examples of digital data include text, images, and videos.

While analog data is more complex to process and manipulate, digital data is much easier to work with due to its binary representation, which allows for more efficient storage, transmission, and processing.

Others

There are many types of digital data, including:

Text data: Textual information, such as emails, documents, web pages, and instant messaging chats.

Audio data: Audio information, such as music files, podcasts, and voice memos.

Image data: Digital images, such as photographs, graphics, and screenshots.

Video data: Digital video, such as movies, TV shows, and home videos.

Sensor data: Data collected by sensors, such as GPS location data, temperature readings, and heart rate monitors.

Transactional data: Data related to transactions, such as sales records, purchase histories, and financial transactions.

Social media data: Data generated by social media platforms, such as tweets, Facebook posts, and Instagram photos.

Machine-generated data: Data generated by machines, such as server logs, sensor data, and automated system data.

Geospatial data: Data that describes the physical location of objects or events, such as maps, satellite imagery, and GPS data.

Behavioral data: Data that describes user behavior, such as website visits, clicks, and online purchases.

## 13.3 Types of Digital Forensics

Digital forensics is a branch of forensic science that deals with the investigation and analysis of digital devices, electronic data, and digital information. There are several types of digital forensics that are commonly used in the field, including:

1. Computer forensics: Computer forensics involves the collection, analysis, and preservation of digital evidence from computer systems, networks, and storage devices. It involves the identification of digital artifacts, such as files, emails, and system logs, and the reconstruction of user activities. This type of digital forensics involves the examination and analysis of computer systems, including hardware and software components, to recover and analyze data.

2. Network forensics: Network forensics involves the investigation of network activity and the reconstruction of events related to digital incidents, such as cyberattacks. It involves the collection and analysis of network traffic data to identify the source of the attack and the extent of the damage.

It involves the analysis of network traffic and communication to investigate security breaches, cyberattacks, and other network-related incidents.

3. Mobile device forensics: Mobile device forensics involves the investigation of data stored on mobile devices, such as smartphones, tablets and other portable electronic devices. It involves the recovery of data from the device's storage, including call logs, messages, emails, and location data.

4. Forensic data analysis: Forensic data analysis involves the examination and analysis of large volumes of data to identify patterns, trends, and anomalies that may be indicative of criminal activity or other types of wrongdoing.

5. Incident response: This type of digital forensics involves the immediate response to a cybersecurity incident or breach, including the identification of the source of the breach and the implementation of measures to prevent further damage.

6. Memory forensics: Memory forensics involves the analysis of the volatile memory of a computer or other digital device. This type of forensics can be used to recover data that has been deleted or encrypted, as well as to identify malicious software and malware.

7. Cloud forensics: The process of investigating digital evidence stored in cloud-based services such as Dropbox, Google Drive, and iCloud. This can involve analyzing server logs, network traffic, and other data to identify potential security breaches or other suspicious activity.

8. Audio and video forensics: This type of digital forensics involves the analysis of audio and video recordings to investigate crimes or incidents, including the enhancement and restoration of degraded or damaged recordings.

9. Database Forensics: Database forensics involves the investigation of data stored in databases. This type of forensics can be used to recover data from a database that has been deleted or altered, as well as to identify unauthorized access or misuse of the database.

These are some of the most common types of digital forensics, but the field is constantly evolving as new technologies and techniques emerge.

## 13.4 Process of Digital Forensics

The process of digital forensics involves a series of steps that investigators follow to identify, collect, analyze, and present digital evidence. The general process of digital forensics includes the following steps:

1. Identification: The first step in the digital forensics process is to identify the devices and digital media that may contain evidence relevant to an investigation. This could involve identifying computers, mobile devices, storage media, and network devices.
2. Collection: Once the devices and media have been identified, the next step is to collect the data from them. This may involve creating a forensic image of the device or media, which is a bit-by-bit copy of the original data. The forensic image is then used for analysis and to preserve the original data.
3. Preservation: It is important to preserve the integrity of the data during the collection process. This involves maintaining the chain of custody of the data and ensuring that the data is not modified or deleted.
4. Analysis: Once the data has been collected and preserved, the next step is to analyze it to identify relevant evidence. This involves searching for files, emails, web browsing history, and other data that may be relevant to the investigation.
5. Interpretation: After analyzing the data, the investigator must interpret the evidence and draw conclusions about what it means in the context of the investigation.
6. Documentation: It is important to document the entire digital forensics process, including the identification, collection, preservation, analysis, and interpretation of the evidence. This documentation may be used in court to support the investigation and prosecution of digital crimes.

7. Presentation: Finally, the evidence must be presented in a clear and concise manner to support the investigation or prosecution. This may involve presenting the evidence in court or to other stakeholders in the investigation.

Overall, the process of digital forensics is a complex and detailed process that requires specialized knowledge and expertise. By following a systematic and scientific approach to digital forensics, investigators can ensure that the evidence collected is admissible in court and can be used to support the prosecution of digital crimes. The process of digital forensics requires specialized skills and tools to be effective. It is important that investigators follow a rigorous and standardized process to ensure the integrity and admissibility of the evidence.

## 13.5 Role of Blockchain Technology in Digital Forensics

Blockchain technology can play an important role in digital forensics by providing a tamper-proof and transparent way to store and track digital transactions and data. Here are some ways blockchain technology can be useful in digital forensics:

1. Immutable data storage: Blockchain technology allows for the creation of a decentralized and immutable ledger that records every transaction and change made to it. This can be useful in digital forensics, where the integrity of data and evidence is crucial. By storing data on a blockchain, investigators can be confident that the data has not been tampered with and can be trusted as evidence.
2. Chain of custody: Blockchain technology can provide a secure and transparent chain of custody for digital evidence. By recording each transfer of the evidence on the blockchain, investigators can track the evidence from the moment it was collected to the moment it was presented in court, ensuring its admissibility.
3. Traceability: Blockchain technology can provide traceability for digital assets, such as cryptocurrencies or other digital tokens. This can be useful in cases where digital assets have been used in criminal activities, such as money laundering or cybercrime. By tracing the flow of digital assets on a blockchain, investigators can identify the source and destination of the funds and use that information as evidence.
4. Forensic analysis: Blockchain technology can also be used in forensic analysis of digital evidence. By analyzing the data stored on a blockchain, investigators can uncover patterns and relationships between transactions and identify potential criminal activities.

Overall, blockchain technology can provide a secure and transparent way to store, track, and analyze digital evidence. While it is not a panacea for all digital forensic challenges, it can be a valuable tool for investigators in certain cases.

## 13.6 Overview of National Cyber Security Policy, 2013

The National Cyber Security Policy was established in 2013, with the purpose of monitoring, safeguarding, and strengthening defenses against cyberattacks. The goal of this policy is to guarantee safe and reliable cyberspace for individuals, organizations, and the government. This Policy aims to protect the information infrastructure in cyberspace, reduce vulnerabilities, develop capabilities to prevent and respond to cyber threats, and minimize damage from cyber incidents through a combination of institutional structures, processes, technology, and cooperation.

### Need for the National Cyber Security Policy:

India lacked a cybersecurity policy before 2013. It was felt to be necessary amid the 2013 NSA surveillance scandal. People are empowered by information, thus it's important to distinguish between information that can move freely between systems and that needs to be secured. These could include private information, banking and financial information, and security information that, if it falls into the wrong hands, could endanger the safety of the nation. Therefore, the government must be able to foster public confidence in the Information and Communications

Technology (ICT) systems that oversee financial transactions if it is to digitalize the economy and encourage more digital transactions. In order to cope with the issue of cyber security at all levels, the National Cyber Security Policy document presents a path for developing a framework for a thorough, collaborative, and collective response. The policy acknowledges the necessity of adopting objectives and strategies at both the national and international levels.

- Before 2013, India did not have a cybersecurity policy. The need for it was felt during the NSA spying issue that surfaced in 2013.
- Information empowers people and there is a need to create a distinction between information that can run freely between systems and those that need to be secured. This could be personal information, banking and financial details, security information which when passed onto the wrong hands can put the country's safety in jeopardy.
- This Policy has been drafted in consultation with all the stakeholders.
- In order to digitize the economy and promote more digital transactions, the government must be able to generate trust in people in the Information and Communications Technology systems that govern financial transactions.
- A strong integrated and coherent policy on cybersecurity is also needed to curb the menace of cyber terrorism.

**The Mission of the National Cyber Security Policy, 2013:**

- To protect information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

**The Objective of the National Cyber Security Policy, 2013:**

- Encourage organized IT systems in all the sectors of the economy for a more secure cyber ecosystem. Also, strengthen more administrative framework for secured cyberspace.
- To create cyber policies in compliance with the global security standard. Best international standard to be followed for infrastructure technology, people, and process.
- To enhance and develop indigenous cyber security technology, by operating a 24X7 National Critical Information Infrastructure Protection Centre (NCIIPC) and making it mandatory security practices related to the design, acquisition, development, use, and operation of information resources.
- Build manpower of 500,000 cyber security skilled professionals in the next 5 years of time.
- Provide Fiscal benefits to businesses that embrace standard security practices and processes. Ensure appropriate legislative intervention during the prevention, investigation, and Prosecution of cybercrime.
- Designate a National nodal agency with clearly defined roles and responsibilities for coordination of matters related to Cyber Security in the country.
- All Private and public organizations must hire Chief Information Security Officer in their IT department.
- These organizations must develop information security policies based on their business requirement. Assure that the IT infrastructure is built in conformity assessment and certification of compliance to cyber security best practices, standards, and guidelines like ISO 27001 ISMS ISO 27001 ISMS certification, IS system audits, Penetration testing/ Vulnerability assessment, application security testing, and web security testing.

- National Level Computer Emergency Response Team (CERT-In) to operate as Nodal agency for Cyber security emergency response and Crisis Management. It will function as an umbrella company of sectoral CERT.
- To collaborate on Research & Development projects with industry and those who develop technologies and solution-oriented research.
- Maintain bi-lateral and multi-lateral relationships with other countries' cyber security teams.
- Strengthen National and Global corporations amongst security agencies, CERTs Defence agencies and forces, Law enforcement agencies, and the Judicial system.

**Cause of Concern of the National Cyber Security Policy, 2013:**

Many more challenges are rising every day with the rise in dependability on cyberspace.

- Concerns about increased cyberattacks from China and its close allies have grown as a result of the standoff at the border. Advisories published by the 'Indian Computer Emergency Team' and media about the possibilities of cyber-attacks from China
- There have been reports that one-third of all worldwide cyber-attacks are executed from China. They are currently working on technologies that would allow them to access the internet through satellite channels.
- APT 36 is being used by Pakistan to target Indian companies. In fact, there is a hacker group called LAZARUS that is well known for carrying out attacks on financial targets in India, Bangladesh, and other South Asian countries.
- Malware, or malicious software, can be used to sabotage computer operations as well as to steal, encrypt, or delete critical data. The Nuclear Power Corporation of India Ltd, which manages nuclear reactors all over the nation, has already faced one such attack.
- WhatsApp filed a lawsuit against Israeli surveillance company NSO Group, alleging that the company assisted clients in employing spyware to gain access to the phones of over 1,400 users, including those in India. Journalists and dissidents were among the targets of the cyberattack.

## 13.7 Cyber Laws Applicable in India

### Cyber Laws

There are several cyber laws that are applicable in India. Some of the major ones are:

1. The Information Technology Act, 2000: This is the primary law governing all electronic transactions and digital data in India. It provides legal recognition for electronic documents and signatures, and includes provisions for data protection, cyber-crimes, and penalties for offenses related to computer systems.
2. The Indian Penal Code, 1860: This is the main criminal law in India, which has been amended to include provisions for cyber-crimes. Sections 65 to 75 of the IT Act, which deal with cyber-crimes, are also included in the Indian Penal Code.
3. The Indian Copyright Act, 1957: This law governs the protection of copyrights in India, including those related to digital content such as music, software, and movies.
4. The Information Technology (Intermediaries Guidelines) Rules, 2011: These rules provide guidelines for internet intermediaries such as social media platforms and internet service providers. The rules require intermediaries to remove illegal or objectionable content within a specified time frame.

5. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016: This law establishes a unique identification system for Indian residents, known as Aadhaar, and regulates the collection and use of Aadhaar data.
6. The Right to Information Act, 2005: This law provides citizens with the right to access information held by public authorities, including digital records.
7. The Personal Data Protection Bill, 2019: This bill, which is yet to be passed into law, seeks to regulate the collection, use, storage, and sharing of personal data in India. It includes provisions for data protection, cross-border data transfers, and penalties for non-compliance.

These laws are designed to protect the interests of citizens and businesses in India, and to promote the growth of the digital economy while preventing cyber-crime and ensuring data protection.

### Cyber Regulations

Some of the top cybersecurity regulations in India are:

1. The Information Technology (IT) Act, 2000: This act provides a legal framework for electronic transactions and digital data. It includes provisions for data protection, cyber-crimes, and penalties for offenses related to computer systems.
2. The Indian Cyber Crime Coordination Centre (I4C): The I4C was established by the Ministry of Home Affairs in 2018 to deal with cyber-crime in India. It is responsible for coordination among law enforcement agencies, public and private sector organizations, and international organizations for investigating cyber-crime and for creating public awareness about cyber security.
3. The Reserve Bank of India (RBI) Cyber Security Framework: The RBI has issued guidelines for banks and other financial institutions to enhance their cyber security. The guidelines require banks to set up a cyber-security framework to identify, detect, protect, respond, and recover from cyber incidents.
4. The National Cyber Security Policy 2013: The policy aims to build a secure and resilient cyberspace for citizens, businesses, and the government. It includes measures to develop human resources, create awareness about cyber security, establish a cyber-security ecosystem, and promote research and development in the field of cyber security.
5. The Personal Data Protection Bill, 2019: This bill seeks to regulate the collection, use, storage, and sharing of personal data in India. It includes provisions for data protection, cross-border data transfers, and penalties for non-compliance.
6. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These rules were recently introduced to regulate intermediaries such as social media platforms, OTT (over-the-top) platforms, and digital news media. The rules require intermediaries to establish a grievance redressal mechanism, comply with the Code of Ethics, and appoint a grievance officer.

These cybersecurity regulations in India are designed to protect the interests of citizens and businesses in India and promote the growth of the digital economy while preventing cybercrime and ensuring data protection.

**Do you know?**

What is Cyber Crime Investigation Cell (CCIC)

The Cyber Crime Investigation Cell (CCIC) is a specialized unit within law enforcement agencies that is responsible for investigating cybercrime cases. The CCIC's primary objective is to investigate and prosecute criminal activities that involve the use of digital technologies and the internet.

The CCIC team comprises law enforcement officials who have specialized training in digital forensics, computer science, and cybercrime investigation techniques. They work closely with other government agencies, including computer emergency response teams (CERTs), intelligence agencies, and prosecutors, to ensure that cybercriminals are brought to justice.

Some of the key responsibilities of the CCIC include:

- Conducting investigations into cybercrime cases, such as hacking, identity theft, phishing, cyberbullying, and cyberstalking.
- Collecting and analyzing digital evidence from computers, mobile devices, and other digital devices to identify and track suspects.
- Collaborating with other law enforcement agencies, both domestic and international, to exchange information and coordinate investigations.
- Developing and implementing strategies to prevent cybercrime and protect critical infrastructure from cyber-attacks.
- Educating the public and businesses on cybersecurity best practices to minimize the risk of becoming a victim of cybercrime.

## Summary

The National Cyber Security Policy of India was launched in 2013 with the aim of safeguarding the nation's cyberspace and ensuring a secure and resilient cyber ecosystem. The policy has the following key objectives:

**Creating a secure cyber ecosystem**: The policy aims to create a secure cyber ecosystem by promoting the development of secure infrastructure, encouraging the adoption of best practices in cyber security, and building the capacity of stakeholders to deal with cyber security threats.

**Strengthening the regulatory framework:**The policy aims to strengthen the legal and regulatory framework for cyber security by creating effective laws and regulations, establishing institutions to enforce them, and promoting international cooperation in the area of cyber security.

**Promoting research and development:**The policy aims to promote research and development in the field of cyber security by supporting the development of innovative technologies, encouraging collaboration between industry and academia, and promoting the sharing of best practices and knowledge.

**Building a skilled workforce:**The policy aims to build a skilled workforce in the area of cyber security by promoting training and capacity building programs, encouraging the development of specialized courses in cyber security, and promoting the recruitment of cyber security professionals.

**Promoting awareness:**The policy aims to promote awareness of cyber security among stakeholders, including citizens, businesses, and government agencies, by launching awareness campaigns, promoting the adoption of best practices, and providing information and resources on cyber security.

The National Cyber Security Policy of India is an important step in securing the nation's cyberspace and protecting its citizens, businesses, and critical infrastructure from cyber security threats. The policy reflects the government's commitment to creating a secure and resilient cyber ecosystem and promoting the development of a skilled and capable workforce to deal with the evolving cyber security landscape.

The CCIC is a vital component of the law enforcement agency's efforts to combat cybercrime and ensure that cybercriminals are brought to justice.

## Keywords

Anti-Forensics Techniques: Techniques used by individuals or organizations to prevent or hinder digital forensic investigations. This can include encryption, data destruction, and other methods used to conceal or destroy evidence.

Cloud Forensics: This type of digital forensics involves the investigation of data stored in cloud computing environments, including cloud storage and software-as-a-service platforms.

Computer Forensics: The application of forensic techniques to the investigation of digital evidence in order to identify, collect, analyze, and preserve information that is relevant to a legal or regulatory investigation.

Cybercrime: Cybercrime refers to criminal activities that are committed using the internet, computer networks, or other forms of digital communication technology. Some common examples of cybercrime include hacking, identity theft, phishing scams, cyberbullying, online harassment, and distributed denial-of-service (DDoS) attacks.

Cybersecurity Investigations: The process of investigating potential security breaches or other cybersecurity incidents in order to identify the source of the activity and take steps to prevent further damage.

Cyber Threat Intelligence: The process of gathering and analyzing information about potential cyber threats in order to identify trends, predict future attacks, and develop proactive security measures.

Cybercrime Investigations: The process of investigating crimes committed using the internet or other digital technologies. This can include a wide range of offenses such as hacking, identity theft, fraud, and distribution of illegal content.

Data Acquisition and Preservation: The process of collecting and preserving digital evidence in a manner that is admissible in court and complies with legal and regulatory requirements.

Data Recovery: The process of recovering data that has been lost or deleted due to accidental deletion, hardware failure, or other causes. This can involve using specialized software tools to recover data from damaged hard drives or other storage media.

Digital Evidence Analysis: The process of examining and analyzing digital evidence to extract information and draw conclusions that can be used in a legal or regulatory investigation. This can include examining hard drives, email accounts, social media profiles, and other digital media.

File Carving: The process of extracting individual files or fragments of files from damaged or corrupted storage media. This can involve analyzing the structure of the storage media and using specialized software tools to identify and recover individual files.

Malware Analysis: The process of analyzing and reverse engineering malware in order to understand how it works and how it can be detected and removed. This can involve examining the code of the malware, running it in a controlled environment, and analyzing its behavior.

Memory Forensics: The process of investigating the contents of a computer's RAM in order to identify active processes, network connections, and other information that may be relevant to an investigation.

Mobile Device Forensics: The process of investigating digital evidence on mobile devices such as smartphones and tablets. This can involve analyzing call logs, text messages, emails, social media activity, and other data stored on the device.

## SelfAssessment

1. What is digital data?

A. Information that is recorded and stored electronically.

B. Information that is recorded and stored on paper.

C. Information that is recorded and stored on a magnetic tape.

D. Information that is recorded and stored on a CD.

2. Which of the following is not a source of digital data?

A. Social media

B. Internet browsing history

C. Printed books

D. Online purchases

3. Which of the following is an example of structured data?
A. Tweets on Twitter
B. Facebook posts
C. Sensor data from a weather station
D. News articles

4. Which of the following is an example of unstructured data?
A. A spreadsheet containing sales data
B. A database of customer information
C. A collection of emails
D. A digital photograph

5. Which of the following is not a challenge of managing digital data?
A. Ensuring data privacy and security
B. Dealing with data overload
C. Storing data in a physical format
D. Maintaining data accuracy and integrity

6. Which of the following sources of digital data is used for scientific research?
A. Social media posts
B. Online customer reviews
C. Sales data from e-commerce websites
D. Weather data collected by sensors

7. Which of the following sources of digital data is used for targeted advertising?
A. Publicly available datasets
B. Online search histories
C. Scientific research databases
D. Digital maps

8. Which of the following is NOT a source of digital data?
A. Social media platforms
B. IoT devices
C. Radio signals
D. Television signals

9. Which type of digital forensics involves the analysis of data stored in cloud-based services?
A. Forensic Data Analysis
B. Incident Response
C. Cloud Forensics
D. None of the above

10. Which type of digital forensics involves analyzing the volatile memory of a computer system?

A. Computer Forensics
B. Mobile Device Forensics
C. Network Forensics
D. Memory Forensics

11. Which type of digital forensics involves the analysis of network traffic data?
A. Computer Forensics
B. Mobile Device Forensics
C. Network Forensics
D. Memory Forensics

12. Which type of digital forensics involves the analysis of data found on smartphones and tablets?
A. Computer Forensics
B. Mobile Device Forensics
C. Network Forensics
D. Memory Forensics

13. Which type of digital forensics involves the analysis of digital data found on computers, laptops, and servers?
A. Computer Forensics
B. Mobile Device Forensics
C. Network Forensics
D. Memory Forensics

14. Which Indian agency is responsible for cybercrime investigation and forensics?
A. Central Bureau of Investigation (CBI)
B. National Investigation Agency (NIA)
C. Cyber Crime Investigation Cell (CCIC)
D. None of the above

15. Which authority is responsible for implementing the provisions of the Information Technology Act, 2000?
A. Ministry of Electronics and Information Technology
B. National Cyber Security Coordinator
C. Cyber Appellate Tribunal
D. All of the above

## Answers forSelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | A | 2. | C | 3. | C | 4. | D | 5. | C |
| 6. | D | 7. | B | 8. | C | 9. | C | 10. | D |
| 11. | C | 12. | B | 13. | A | 14. | C | 15. | A |

## Review Questions

1. Discuss the sources and types of Digital Data.
2. Explain the types of digital forensics.
3. Explain the process of digital forensics.
4. Discuss the role of blockchain technology in digital forensics.
5. Explain the need and mission of the National Cyber Security Policy, 2013.
6. Give the objective of the National Cyber Security Policy, 2013.
7. Discuss the cause of concern of the National Cyber Security Policy, 2013.
8. Discuss the cyber laws applicable in India.
9. Discuss the cyber regulations applicable in India.

## Further Readings

- https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf#:~:text=1)%20To%20create%20a%20secure,all%20sectors%20of%20the%20economy.
- https://www.geeksforgeeks.org/the-national-cyber-security-policy-2013/

# Unit 14: Fraud Management

CONTENTS



## Objectives

After studying this unit, you will be able to:

- discuss the consequences of corporate fraud.
- examine the conceptual model for culmination of corporate fraud.
- explain the policy implications of corporate fraud.

## Introduction

Corporate frauds have acquired an undesirable but inevitable presence in India's economy which is posing a threat to the economy. These have shown an unprecedented increase in India in recent years and the reason for the enormous increase in frauds is to be found in the fast-developing economy and industrial growth of this developing country. It is seen that globally corporate frauds are increasing and accordingly new and new legislations are being enacted. The fraud problem is probably more serious in rich countries. Poor country's governments probably accept more bribes and commit more offences, but it is rich countries that host the global companies that carry out the largest offences.

Various legislative measures, with a sectoral focus, deal with fraud and corruption in public domain. The Securities and Exchange Board of India, the Reserve Bank of India, the Serious Fraud Investigation Office, the Company Law Board, the Central Vigilance Commission, the Economic Offences Wing, the Income Tax department of the Central Government, and various courts are major regulatory authorities under different statutes which seek to prevent and detects frauds and punish the guilty.

Although the Indian regulatory and legal system is well-designed and quite comprehensive, but inefficient in implementation and handling of the corporate frauds both from definitional and strategic handling perspective. Conventional wisdom holds that more litigation is better when it comes to combating corporate frauds. However, this wisdom doesn't reflect the modern reality of corporate frauds litigation. Fraud can be prevented by securing processes and by ensuring that people allowed access is honest. Efforts are being made by all concerned to prevent such corporate frauds and alienate the pain and agony of small investors and shareholders. Regulatory agencies/authorities in India are increasingly identifying possible corporate frauds risks and becoming proactive in their actions.

Further increased cooperation between regulatory authorities in different countries has given rise to a new trend in enforcement. For example, financial intelligence unit, in India has joined the Egmont Group to tackle the money laundry. The enforcement machinery is improving in the country but they still lag behind other countries in measures and combat corporate frauds.

## 14.1 Overview of Fraud Management

Fraud management refers to the process of preventing, detecting, and responding to fraudulent activities that can occur in a business or organization. The goal of fraud management is to minimize the risks and damages that result from fraudulent activities, such as financial losses, legal issues, damage to reputation, and loss of customer trust.

The process of fraud management typically involves several steps, including:

Risk assessment: Identifying the areas of the business that are most vulnerable to fraud and assessing the likelihood and potential impact of fraudulent activities.

Prevention: Implementing measures and controls to reduce the risk of fraud, such as employee training, background checks, access controls, and fraud detection software.

Detection: Monitoring for suspicious activities and transactions, using tools such as data analytics, transaction monitoring, and employee tips.

Investigation: Conducting investigations into suspected fraudulent activities to determine the scope, cause, and impact of the fraud.

Response: Taking action to address the fraud, such as recovering lost funds, terminating employees involved in the fraud, and implementing new controls to prevent future fraud.

Effective fraud management requires a proactive and comprehensive approach that involves all levels of the organization, from senior management to front-line employees. It also requires a commitment to ongoing monitoring and continuous improvement to stay ahead of evolving fraud threats.

### Stages of Fraud Management

Fraud management typically involves several stages, which may vary depending on the organization and the nature of the fraud risk. The following are the general stages of fraud management:

Prevention: This stage involves implementing measures to prevent fraud from occurring. These measures may include security controls, training and awareness programs, internal controls, and monitoring systems.

Detection: This stage involves detecting potential fraudulent activity through various methods, such as data analysis, internal and external audits, and tip-offs from employees or third parties.

Investigation: Once potential fraud is detected, an investigation is initiated to gather evidence and determine the extent of the fraud. This stage involves interviewing employees and third parties, reviewing documents and data, and conducting forensic analyses.

Resolution: This stage involves taking appropriate action to resolve the fraud, which may include disciplinary action, legal action, or recovery of losses.

Monitoring: This stage involves implementing ongoing monitoring and controls to prevent similar fraud from occurring in the future. This stage may also involve assessing the effectiveness of fraud prevention and detection measures and making necessary improvements.

## 14.2 Consequences of Corporate Fraud

### Consequences of Fraud on Company's Stakeholders

The consequences of corporate frauds on the stakeholders can be assessed in of default in the payment to creditors, loss of confidence among the investors, loss of credibility of the company, and the low of experienced employees due to their switching over. The major consequences of corporate fraud on stakeholders, i.e shareholders, creditors, investors, bankers, financial inclinations, vendors and employees, are stated below:

1. Loss of confidence of investors in the organization
2. Loss of credibility of the organization
3. Loss of employees due to switching over
4. No-payment to credits
5. Non-payment to bankers against working capital facilities availed leads to NPA which damages bankers
6. Non-receiving of dividend for long period
7. Loss of capital invested by investors (Indian and Foreign investors)
8. Decrease in value of investment
9. Employees losses their savings and pension

It is noteworthy that the non-payment to creditors restricts the foreign entities to apply the goods to the organization, and loss of confidence of investors leads to reduction in investment by foreign investor. The major consequence of a corporate fraud on stakeholders is the decrease in value of their investment as a corporate fraud significantly increases the company's losses due to poor financial performance.

### Consequences of Fraud for the Organization

The consequences of a corporate fraud on the organization are loss of cab fa assets, reputation, sales, and decrease in value of shares, adverse effects banker's attitude, unrealistic corporate targets, insider-trading, overstating pr and productivity growth

It is inferred that the fraud has the financial implications, adversely affects t reputation and lowers the employee's morale. The financial implications include the loss of funds, lowering of share prices, and borrowings at higher cost. The reputational implication includes the impact on ability and reliability of organization, which deter future clients. The employees' moral implications include the damages to the trust of the employees, future recruitment and te retention of existing staff. The major consequences of corporate fraud organizationare: -

1. Adverse effect on banker's attitude in respect of granting of loans and other credit facilities
2. Loss of assets (current and fixed)
3. Loss of Net worth
4. Lots of Reputation/Goodwill of the company
5. Loss of sales leads to decrease in revenue
6. Loss of dedicated and experienced employees
7. More government regulations
8. Decrease in value of shares
9. Loss of confidence of investors (Indian and Foreign)
10. Bound to set unrealistic corporate targets
11. Decrease in productivity growth
12. Lowering of employee's morale
13. Loss of customers (existing and future) due to negative publicity media

### Consequences of Fraud for the Economy

The impacts of corporate frauds on the economy are higher cost, slower gr and reduction in employment, increased government control, and adverse eft on overall growth of the country. The major consequences of corporate frauds on the economy are imposition of increased government controls, higher cost of projects and loss of confidence of foreign investors, which in turn lead to slower growth of the economy and reaction in employment opportunities. From a broader perspective, corporate frauds create immense negative impact on the investment climate in the country. The major impact of Corporate Frauds in the economy on a whole are:

1. Adverse effect on overall growth of the country
2. Loss of confidence of foreign investors
3. Higher cost of projects

4. Imposition of more government controls
5. Reduction in employment
6. Negative impact on the investment climate in the country
7. Loss of Revenue due to stripping of large taxes
8. Negative plunge on national wealth
9. Adverse effect on the Foreign Exchange
10. Citizens have to pay more for their goods
11. Government bound to put taxes on higher side
12. Inadequate or false returns affects policy making and implementation

The complexity of a Corporate Fraud (which is the handy work of a select few) comes bare only when the complete edifice of a company has collapsed. All of a sudden, we hear that a company has cheated the gullible investors and that the directors of the company have gone underground. This shakes up the confidence of all the stakeholders; and the shareholders are helpless before a corporate mammoth. Such a corporate fraud strips of the large taxes, which the government could have earned, it strips of the valuable savings of the investors and the National Wealth has a negative plunge and everybody seems bewildered. There is an urgent need for uniformity of publication standard of fraud prevention policy.

The detection of corporate frauds many a times becomes difficult since the financial statements are fabricated or the balance sheet is camouflaged and also the frauds are never a part of directors' report. The statutory disclosures also give statements on such camouflaged balance sheet; hence there appear to be a close and strong nexus between the perpetrators of the fraud and the unscrupulous professionals, making the fraud invisible till the lid blows off. The curse of corporate frauds has a silver lining in the cloud, as there are simple methods, which can be evolved to deter the perpetrators of the white-collar crime, its timely detection and punishment of the accused and the delinquent persons.

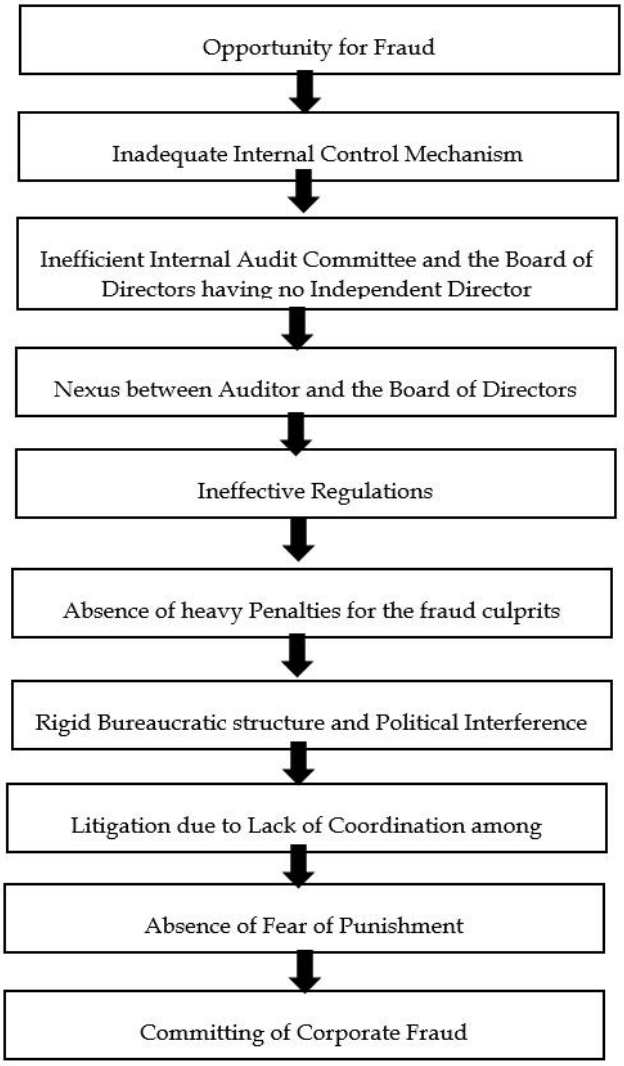
To avoid the severe consequences, the management and government have to take effective steps to curb frauds. It can be undertaken at three key levels: the corporate level, work group level, and the individual level. A beginning step in this respect is to engage psychologists to administer personality tests and rating scales on new employees, with emphasis on issues of integrity. These usually consist of a sizeable array of emotional, social, and attitudinal variables. The reward system should focus on ethical performance, integrity, responsibility self. leadership on the job, and standards-linked incentives. Moreover, there should be a commitment from the top management to mitigate inequities, nepotism and sectionalism, if any exists in the organization. Besides, the management should promote objectivity and transparency in the staff performance appraisal system and put strong emphasis on behavioral attributes linked with the values of corporate excellence. There is a need to review the corporate values and the prevailing way of life in the organization. This may require a systematic diagnosis of the cultural alignment with the strategic situation of the organization.

The norms and values relating to self-managed high-performance, and team responsibility as well as strategic mentoring must be considered.

## 14.3 Conceptual Model for Culmination of Corporate Fraud in India

Corporate governance issues are important for the international business community and financial institutions. In the corporate sector in India, there is considerable weakness in the proper corporate governance and regulatory mechanism which needs amendment in the existing regulatory framework. There is a time lag between the actual occurrence of a fraud and the information reaching the public domain, and public interest is adversely affected by such delay. The appointment of qualified and independent directors in the audit committees will also help in preventing or minimizing frauds. The rotation of statutory auditors and compulsory appointment of qualified internal auditors would also tend to prevent frauds. For such changes, there is an urgent need for reframing and amending the existing legislations as some of them old and outdated. The auditors also need to be trained in order to make them well-equipped with the changed regulatory measures and technological advancements.

A conceptual Model for Culmination of Corporate Fraud




Source: Gupta, D. S. (2016). Corporate Frauds & their Regulation in India (First ed.). Bharat Law House PVT. LTD.

## 14.4 Policy Implications of Corporate Fraud

It is not possible to eliminate frauds in the corporate sector as no system is completely 'fraud proof. However, if an organization or government pay greater attention to the most common indicators, they can provide early warning to discover the fraudster and to prevent the fraudster from committing a fraud.

Therefore, the corporate frauds can be minimized by adopting certain policies by the organization and stakeholders. The Companies Act, 2013 has covered many points to minimize the frauds in the corporate sector but still some are missing from it. The following policy implications can be benefitted for reducing corporate frauds in India:

### Strengthening of the Internal Audit Department and Audit Committees

The internal audit department needs to be strengthened by appointing qualified and experienced personnel. The Companies Act and listing agreements of different Indian stock exchanges provide for the constitution of an audit committee. However, no qualification or experience of such members has been prescribed. Due to lack of their knowledge and experience, frauds are often committed by companies' despite of comply with the provisions of different statutes. It is suggested that the Audit Committees should be given the freedom to act independently from the executives, and at least one of the members of the Internal Audit Committee should have recent and relevant financial knowledge and relevant experience.

### Implementation of Corporate Governance in Small and Medium Enterprises (SMEs)

The Small and Medium Enterprise sector is the second largest employer, after agriculture. The applicability of Corporate Governance in SMEs may have the way for the companies to grow or attract additional investors as alternatives to borrow from Bank at higher cost. The Corporate Governance in their sector may improve internal control system, better accountability and higher profitability and it will also reduce the conflicts between business owners and management.

### Adoption of International Financial Reporting Standards (IFRS)

The Indian economy is at developing stage where foreign entities are partners with Indian entities, so proper disclosures in the financial reports are required on globally accepted disclosure standards, therefore, it is suggested to introduce IFRS in each class of companies mandatorily and a strengthening of reporting regulation would probably ease out the process of corporate frauds controlling.

Beside this, stricter disclosure to Stock Exchange related to sale/ purchase of shares by the controlling group as well as stricter surveillance by SEBI may prevent Corporate Fraud.

### Conducting Due Diligence effectively by Banks and Financial Institutions

Banks and Financial Institutions are the major stakeholders in companies as finances are provided by them. To safeguard their interest, banks and financial institutions have to effectively conduct due diligence by independent professionals and agencies before sanctioning the working capital facilities or other financial assistance to the companies.

### Appointment of Independent Professionals by Shareholders and Fixing of their Responsibility

The present legislation has given power to the board of directors and to so called shareholders to appoint auditors and other compliance professionals. The Institute of Chartered Accountants of India should issue guidelines to its members who work as Statutory Auditors, Auditors, Chief Financial Officer and Corporate consultants to ensure giving of proper disclosures in structured deals where money flows from one end to another which goes back to an entity connected with the director of the company.

### Setting up of Corporate Offence Wing with Criminal Powers

Presently, there is no specific authority which exclusively deal with corporate frauds. It is suggested to form a Corporate Offence Wing on the parallel line of Economic Offence Wing to prevent and detect the corporate fraud and to punish the offenders and conspirators who are involved in committing corporate frauds.

### Approval of Related-Party Transactions by Specific Committee

The Companies Act, 2013 removed the approval of Central Government for related party transactions in those companies which have paid-up capital of Rs. 1 Crore or more. The Act contains the provisions for related-party transactions but only shareholders' approval is required. It is suggested that a separate specific committee consisting of one independent director and one minority shareholder representative has to be formed by each company for approving the related-party transaction, subject to the approval of shareholders as these transactions are camouflaged by raising debit/credit note to give a favorable price to related party.

### Publication of Fraud Prevention Policy

Non-existence of uniformity of publication standard of fraud prevention policy attracts the suggestion that a publication of uniform fraud prevention policy should be made mandatorily by certain class of companies and it has to be discussed at length in board of director's report of the company. The fraud prevention policy must be publicized among the employees and stakeholders of the company and make mandatorily to report suspected frauds through a well-structured mechanism.

### Recognition to Companies for Improved Corporate Governance

Good corporate governance is one of the major factors for the economic success of companies. Corporate governance has an impact on the profitability, growth and sustainability of business. Clause 49 of listing agreement deals with corporate governance. The Institute of Company Secretaries of India (ICSD for the last several years awarding companies for better corporate governance, it is suggested that government or other authorities should also encourage by giving awards to corporate as well as professionals to adopt better corporate governance which will ultimately affect the growth and sustainability of business.

### Co-ordination among different Regulatory Authorities

Regulatory agencies/authorities in India are increasingly identifying possible corporate frauds risks and becoming proactive in their actions and recently the Government of India constituted the Competition Commission of India to preview antitrust and monopolistic risk prior to large merger and acquisition as well as during operations. The Reserve Bank of India has also stepped up of enforcement of anti-money laundry regulations. Proper coordination among numerous regulatory authorities is recommended.

## Summary

Corporate frauds can have a devastating effect on the business firm in which the fraud has occurred. Such effect on the organization is due to the fact that an individual who is employed by the organization has knowledge of the financial system, as well as company's confidential information, and is able to manipulate them over a period of time. These individuals also have a working knowledge of the various counter-frauds, counter intelligence, and security procedures, which have been established, and can find ways and methods to circumvent the counter-fraud and security counter measures, which have been put in place.

The loss in the organization can also have an impact on the local, state or national economic conditions based on the size of the business affected by the fraud. With the lack of policy in an organization's business, there is an inherent lack of control. This can be the lack of control of systems, programs and even people.

When a company suffers a loss from fraud, it would make up for it by raising the costs, which ultimately means higher prices for consumers. It can also mean less pay for employees and even cutting of jobs. The effect can continue to ripple when it comes to those employees or investors who now find themselves unable to pay off the loans, and the credit becomes harder to obtain.

The fraud can also have a social impact on the organization. It can allow the organization to lose the confidence of the company's stockholders. It can also contribute to a loss of confidence in the organization by its advertisers. The negative publicity from the media can also impact how the organization is perceived and supported by the community in which the organization operates as well as its customer-base. The cumulative effect on all of the negative circumstances may also have a major impact on the organization's reputation and stock value which often lead to the closure of the business or an unprecedented loss of revenue.

Any person or organization can be affected by a financial statement fraud that has an interest in the success or failure of a company. A bank that gives credit to the company, a shareholder who invests money in the company, and the organization that enters into a contract or agreement with the company, all can be affected if there is a manipulation in the company's reported earnings or assets. Employees can also be affected by the manipulation in the financial statement. It has the power to put employees out of work once the fraud is exposed. Good financial results (actual or fabricated) can be linked to promotions, enhanced salary and benefit packages, bonus, and the value of stock options.

Financial statement fraud will cause shareholders to overpay for their investment in the company and to get less value for their money. Shareholders may lose part or all of their investment if the company fails or has to go through some sort of re-organization. Financial statement fraud directly harms the investors and the creditors who lose all or part of their investment if such fraud results in bankruptcy, failure, reduction in the stock prices or delisting by the Stock Exchanges. Financial fraud can also have an adverse impact on the confidence and the trust of investors, other market participant and the public in the quality and integrity of the financial reporting process. Users of financial statements will lose because of their wrong financial decision (e.g. non-investment in the case of investors made on unreliable), and misleading financial information. Financial statement fraud contributes to considerable economic loss by investors and creditors.

## Keywords

Fraud: An intentional act of deception, misrepresentation, or concealment to gain unauthorized access to assets, information, or services.

Management: The process of planning, organizing, directing, and controlling resources to achieve organizational goals and objectives.

Prevention: The act of taking steps to stop fraud from occurring or reduce the likelihood of it occurring.

Detection: The process of identifying or uncovering fraudulent activity, often through monitoring or analysis of data.

Investigation: The process of gathering evidence and conducting inquiries to determine the extent and nature of fraudulent activity.

Resolution: The actions taken to address and resolve fraudulent activity, including disciplinary action, legal action, and recovery of losses.

Monitoring: The process of ongoing surveillance and evaluation to ensure that fraud prevention and detection measures are effective and that fraudulent activity is promptly identified and addressed.

Risk Management: The process of identifying, assessing, and managing risks associated with fraud and other potential threats to an organization's assets, reputation, and operations.

Internal Controls: The policies, procedures, and mechanisms put in place to ensure that an organization's assets are protected and that fraud is detected and prevented.

Compliance: The process of ensuring that an organization adheres to legal and regulatory requirements related to fraud prevention, detection, and reporting.

## SelfAssessment

1. What is fraud management?

A. A process to prevent all types of fraud

B. A process to detect, investigate and resolve fraud

C. A process to manage an organization's finances

D. A process to improve employee performance

2. What is the primary goal of fraud prevention?

A. To eliminate all fraud risk

B. To reduce the likelihood and impact of fraud

C. To detect fraud quickly

D. To prosecute fraudsters

3. Which of the following is an example of fraud detection?

A. Implementing strong passwords

B. Providing regular fraud awareness training

C. Conducting background checks on employees

D. Monitoring transactions for suspicious activity

4. What is the first step in fraud investigation?

A. Collecting evidence

B. Interviewing witnesses

C. Reporting the fraud to law enforcement

D. Conducting a risk assessment

5. Which of the following is a common type of fraud resolution?

A. Implementing new internal controls

B. Terminating the employment of the fraudster

C. Filing a lawsuit against the fraudster

D. All of the above

6. What is the potential impact of corporate fraud on a company's reputation?
A. It can enhance the company's reputation and credibility
B. It can have no impact on the company's reputation
C. It can significantly damage the company's reputation and credibility
D. It can lead to the company's bankruptcy

7. What is the potential impact of corporate fraud on employees?
A. It can improve employee morale and motivation
B. It can increase employee job security
C. It can decrease employee morale and job satisfaction
D. It can have no impact on employees

8. What is the potential impact of corporate fraud on shareholders?
A. It can result in an increase in shareholder value
B. It can lead to a decrease in shareholder value
C. It can have no impact on shareholder value
D. It can lead to the company's bankruptcy

9. What is the potential impact of corporate fraud on customers?
A. It can improve customer loyalty
B. It can have no impact on customer loyalty
C. It can significantly damage customer trust and loyalty
D. It can lead to an increase in customer satisfaction

10. What is the potential impact of corporate fraud on regulators and government agencies?
A. It can lead to increased regulation and oversight
B. It can have no impact on regulators and government agencies
C. It can lead to decreased regulation and oversight
D. It can lead to the dissolution of regulators and government agencies

11. What is one of the consequences of corporate fraud?
A. Increased trust in the company
B. Positive impact on the company's reputation
C. Decreased employee morale and engagement
D. Higher stock prices

12. Which of the following is a legal consequence of corporate fraud?
A. Increased revenue
B. Fine or penalty
C. Higher employee retention
D. Greater customer loyalty

13. What is the potential impact of corporate fraud on shareholders?
A. Increased dividends
B. Decreased value of shares

C. Greater confidence in the company
D. Lower risk of financial loss

14. What is one of the consequences of corporate fraud for customers?
A. Improved quality of products or services
B. Decreased prices
C. Reduced trust in the company
D. Greater convenience

15. What is a potential consequence of corporate fraud for the company's senior management?
A. Increased job security
B. Reputation damage
C. Higher salaries
D. Improved public perception

## Answers forSelfAssessment

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. | B | 2. | B | 3. | D | 4. | D | 5. | D |
| 6. | C | 7. | C | 8. | B | 9. | C | 10. | A |
| 11. | C | 12. | B | 13. | B | 14. | C | 15. | B |

## Review Questions

1. Discuss Fraud management.
2. Explain the consequences of corporate fraud.
3. Explain the policy implications of corporate fraud.
4. Describe the conceptual model for culmination of corporate fraud.
5. Explain the consequences of corporate fraud for the economy.
6. Discuss the process of fraud management.

## Further Readings


- Gupta, D. S. (2016). Corporate Frauds & their Regulation in India (First ed.). Bharat Law House PVT. LTD.


### Web Links

- https://seon.io/resources/top-fraud-management-systems-how-to-pick-one/
- https://corporatefinanceinstitute.com/resources/esg/corporate-fraud/

**LOVELY PROFESSIONAL UNIVERSITY**
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in