St. Joseph's Journal of Business Research
E-ISSN-
Vol-1(01)
DOI:

A DESCRIPTIVE STUDY ON FRAUDS IN FORENSIC ACCOUNTING

Pramodini Hansa
PG student-M.COM, St Joseph's University, Bengaluru

St. Joseph's Journal of Business Research
Vol. 1(01), Dec 2022, pp. 12-22

Abstract:
Forensic accounting is used to investigate the fraud, embezzlement and other hidden irregularities in financial transactions. In various situations, forensic accounting investigations are used in legal proceedings. It is also used in order to ensure sufficient compliance are existing to prevent crimes. In this regard, the present descriptive paper explains forensic accounting and the various types of frauds involved in forensic accounting. Some of the concepts were explained with supporting case studies. With the growing concern considering the frauds in banking sector and the recent bankruptcy incidents, various suggestions were propounded to mitigate the frauds to have a good governance and faithful presentation of financial information with a view to protect the interest of the stake holders.
Key words: *Forensic accounting, Fraud, legal proceedings, bankruptcy and cybersecurity.*

Introduction

Accounting, auditing, and investigative abilities are all used in forensic accounting to look into a person's or company's finances. Accounting analysis suitable for use in judicial proceedings is provided by forensic accounting. Forensic accountants are taught to look beyond the statistics and address the situation's commercial realities. In fraud and embezzlement situations, forensic accounting is commonly utilized to explain the nature of a financial crime in court.

Reasons for frauds

A fraud triangle is a forensic auditing technique that outlines three interconnected issues. Components that aid with the commissioning of thievery –

- Constraints (motive),
- Possibility (ability to carry out the task) as well as
- Rationalization (the act of justifying dishonesty)

Conceptual understanding

The application of investigative and analytical abilities for the goal of resolving financial concerns in a manner that meets the standards needed by courts of law is referred to as forensic accounting. Forensic accountants collect, analyze, and assess evidence, as well as interpret and explain results, using unique abilities in accounting, auditing, finance, quantitative methodologies, certain areas of the law, research, and investigative skills (Authors) Kranacher, Riley, and Wells define financial forensic accounting and fraud examination in their book Forensic Accounting and Fraud Examination.

The application of financial principles and theories to facts or hypotheses at issue in a legal dispute is known as financial forensics, and it has two main functions:

1. Litigation advice services, which acknowledges the financial forensic professional's role as an expert or consultant in legal proceedings.
2. Investigative services, which makes use of the financial forensic professional's skills

Types:

Bank Fraud:

As it involves the nation's financial institutions, bank fraud is a white-collar crime that is frequently prosecuted at the federal level. As a result, it carries severe consequences. When facing charges of bank fraud, having the help of an experienced Lincoln and Omaha criminal defense attorney can make all the difference.

Theft of money or assets from a bank, financial institution, or a bank's depositors is classified as bank fraud. Credit unions and banks that are federally insured are considered financial institutions for legal purposes. Federal Reserve banks, the Federal Deposit Insurance Corporation (FDIC), mortgage lending agencies, and other financial institutions that accept money or other financial assets are included.

In general, any premeditated activity aimed at defrauding a financial organization is considered bank fraud. It could entail a deliberate activity aiming at obtaining assets, money, securities, credits, or property from a financial institution by using deception or false information. Bank fraud is defined by the law in a pretty broad sense, and there are various aspects to it.

Bank frauds and their formats

Under federal law, there are several different types of bank fraud that can be prosecuted. The United States Secret Service is in charge of investigating bank fraud and maintaining the security of the country's financial institutions. Every year, the agency fulfills its responsibilities by investigating bank fraud, identity theft, automatic payment system fraud, check forgery and changes, direct deposit fraud, and counterfeiting.

The following are examples of common types of bank fraud:

- Forgery
- Loans that are fraudulent
- Impersonation of a bank
- Checks that have been stolen
- Bank fraud on the internet

When a person changes the name or alters the information on the face of a check, this is referred to as forgery. This could involve adding a zero to the original amount (raising its true value) or fabricating a document.

Corporate fraud

When a multinational corporation's top executives commit corporate fraud, the amount of money involved is frequently in the billions of dollars. Consumers or clients, creditors, investors, rival businesses, and, eventually, the corporation that is the source of the fraud and its personnel are the victims of corporate fraud. When the scam is exposed, the company that perpetrated it is frequently left in ruins and forced to declare bankruptcy.

Much of the money stolen unlawfully through corporate fraud is never retrieved once the criminals have spent it.

Causes of corporate fraud

1. **The desire to recruit or retain investors, or the perception of a need to do so**
   Corporate fraud is frequently committed for the same reason as any other type of fraud: avarice. However, in today's highly competitive global corporate market, it could happen for a variety of reasons. Many corporate fraud schemes use deceptive accounting practices that make a company appear to be more profitable than it is. The desire or perceived necessity to recruit or maintain investors is the driving force behind such programmes.

2. **Issues or flaws in a company's product**
   Another kind of corporate fraud could be hidden flaws or defects in a company's products. Several recent incidents of corporate fraud involving pharmaceutical corporations have been reported.

Insurance fraud

When someone willfully lies to get a benefit or advantage to which they are not otherwise entitled, or when someone knowingly refuses a benefit to which they are entitled, it is called fraud. The crime of insurance fraud can be prosecuted under the law if:

The suspect was out to swindle people. Insurance fraud is a crime with a "specific" intent. This means that the prosecutor must show that the defendant deliberately committed a defrauding act.

A task has been completed. It is sufficient to make a misrepresentation (written or oral) to an insurer with awareness that it is false.

Both the act and the intention must be in sync. It is not a crime to have one without the other.

It is not necessary to experience actual loss as long as the suspect has committed an act and had the intent to commit the crime. No money necessarily has to be lost by a victim.

Kinds of Insurance Fraud and Other Crimes Handled by the Fraud Division

The Fraud Division is responsible for enforcing the provisions of California Insurance Code Chapter 12 (commonly known as the "Insurance Frauds Prevention Act"), California Penal Code Sections 549-550, and California Labor Code Section 3700.5, as well as various felony provisions of the Penal and Insurance Codes. The Fraud Division's investigations usually involve some component of a "Suspected Fraudulent Claim" or other connected offenses.

Criminal activities involving vehicle property and personal injury, workers' compensation, health insurance, and residential and commercial property claims are among the most common cases investigated by the Fraud Division. Some of the types of insurance fraud that are investigated are as follows:

- Automobile Collision
- Automobile Property
- Medical
- Life
- Workers' Compensation
- Fire
- Property
- Healthcare

Cyber Fraud

Cyber fraud is the most widespread and dangerous type of fraud that occurs around the world. Throughout the twenty-first century, the cyber world has expanded and grown, allowing fraudsters to hack victims' personal and financial information in a variety of methods. Fraudsters can use the information which they gather to then financially fund themselves, or worryingly they might use this money to fund terrorism. Therefore, it is essential that individuals and organizations are aware of how to protect themselves against cyber fraud.

The use of the Internet to perpetrate financial fraud, such as phishing emails that collect personal information from unsuspecting readers, counterfeit items for sale on ebay, email scams that claim the recipient is owed money if they perform some transaction for the sender, phony investment schemes, and identity theft. Many of these frauds are merely online versions of off-line scams that have been around for a long time. However, the Internet has provided criminals with access to a global pool of consumer targets as well as increased opportunities to avoid law enforcement because they do not have to be in the same country or even hemisphere as their victims.

Securities fraud

Securities fraud, often known as stock or investment fraud, is a serious white-collar crime that takes many forms but generally involves misleading information that investors use to make decisions.

A stockbroker, for example, could be the perpetrator of the fraud. It could also be a company, such as a brokerage, business, or investment bank. Individuals may commit this form of fraud on their own through techniques such as insider trading.

Securities fraud is a type of unethical or unlawful action that involves the use of securities or asset markets to profit at the expense of others.

This is a serious crime that frequently involves the financial realm.

Securities Fraud: What are the different types of securities fraud?

Securities fraud can take many different shapes. In truth, there are numerous strategies for deceiving investors with incorrect information. For example, high-yield investment fraud may promise high rates of return while saying there is little to no danger. Commodities, securities, real estate, and other types of investments are all possible. Advance fee schemes can take a more nuanced approach, in which the fraudster persuades their victims to advance them small sums of money in exchange for higher returns.

The money is sometimes demanded to cover processing costs and taxes for monies that are supposed to be disbursed soon. Ponzi and pyramid scams often rely on funds provided by new investors to pay off their debts.

Types of security fraud

Securities fraud, also known as stock fraud or investment fraud, happens when a party involved in the purchasing, selling, or trading of a company's stocks gives the public or buyers false information. The incorrect statements have an impact on buyers who are making final financial judgments in the trade industry.

Five of the most typical types of securities fraud are listed here.

1. **Fraudulent high-yield investment**
   Unlicensed individuals commit this form of fraud by operating unregistered investments that offer high rates of return with little or no risk. Victims are frequently contacted through websites created by the offenders. Real estate, equities, commodities, and precious metals are all frequent assets in high yield investment fraud.

2. **Insider trading**
   This type of fraud occurs when a person who has access to a company's secret information utilizes that information to acquire or sell stock. They can use the confidential information to make final financial decisions. An executive who sells his or her stock after learning that his or her company is about to go bankrupt, for example, may be found guilty of insider trading.

3. **Pyramid and Ponzi schemes**
   This sort of fraud occurs when people take money from others with the promise of paying them large rates of return comparable to those paid to previous investors. In actuality, because investors are the main source of money, these schemes can only pay stable returns.

4. **Misrepresentation by a third party**
   When a third party gives incorrect information about a firm in order to attract more people to acquire stock, this is known as insider trading. After the majority of individuals have purchased the stock, the price is more likely to climb, which is when the offender sells their shares for a profit.

5. **Payment plans in advance**
   When a person sends money to an investor expecting to obtain something of greater worth in return, but instead receives little or nothing, they are committing this form of fraud. Furthermore, the criminal may ask the victims to donate money to cover taxes or processing fees.

Consumer fraud

Consumer fraud is described as dishonest commercial tactics that create financial or other harm to customers. When the victims are deceived, they assume they are participating in a lawful and valid business transaction. Consumer fraud is frequently associated with misleading promises or inaccurate claims made to customers, as well as tactics that actually defraud customers of their money.

The Federal Trade Commission considers complaints regarding companies that may have defrauded customers. The agency investigates consumer fraud and unfair business practises in collaboration with law enforcement.

Types of consumer fraud

In 2020, you should be on the lookout for seven major types of consumer fraud. Here's a closer look at these scams to help you spot them and avoid being a victim of consumer fraud.

1. **Theft of one's identity**

You've been a victim of identity theft if someone took your personal information, such as your name, credit card information, or Social Security number. This type of crime is most commonly committed through a technique known as data mining, which is used by many businesses to convert raw data into useful information. Unexpected withdrawals from your bank accounts or bills from medical providers for operations you did not have are common symptoms of identity theft.

2. **Fraudulent use of credit cards**

When someone takes your credit or debit card or gains access to the information on your card, they can use it to make transactions or withdraw money. Credit card charges must total more than $50 to be eligible for dispute under the Fair Credit Billing Act (FCBA). You've most certainly been the victim of credit card fraud if your statement contains transactions you don't recognise, you receive phone calls asking for credit card information, or you notice a large, unexpected fall in your available credit balance.

3. **Scams involving COVID-19**

COVID-19 is an idea for fake news. Consumer fraud can take many forms. The 2020 coronavirus pandemic has resulted in over 239,000 deaths in the United States, as well as millions of job losses and jobless claims. It has also provided scammers with new ways to defraud people. Here are some red indicators to look out for when it comes to possible COVID-19 scams:

- Receiving a phone call, text message, or email advising you about a new remedy or vaccine accessible only from one source;
- Getting a robocall promising financial help; or
- Receiving a call from someone claiming to be from the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO) offering to sell you access to special services or drugs.

4. **Fraudulent Debt Collection**

Scammers who pose as debt collectors deceive consumers. If you have legitimate overdue obligations, the Fair Debt Collection Practices Act protects you (FDCPA). The concealment of facts such as the precise amount of the debt, threats of jail time, and calls very early or late in the day are all common symptoms of debt collection fraud (before 8am or after 9pm).

5. **Reduced Interest Rates Robocalls**

This form of scam, which resembles credit card fraud, is relatively new. It takes the form of automated calls, or robocalls, that promise to lower your credit card interest rate in exchange for a modest charge. After seeking personal information, these types of scammers are known to commit identity theft.

6. **Lottery Scams**

A mousetrap is stacked with a dollar note and a pyramid of coins. There are a few telltale indicators of a phoney lottery fraud. When you receive a phone call, text, or email informing you that you have won a lottery or another type of prize or sweepstakes, you have been the victim of lottery fraud. Requests to pay money to the sweepstakes office to cover taxes or other charges, receiving a "winning" announcement via bulk mail, or being asked to attend a meeting before collecting your prize are all common symptoms of a bogus lottery scam.

7. **Theft of a Mortgage**

Mortgage fraud victims are often troubled homeowners facing foreclosure or another sort of financial hardship relating to their home. Promises of loan modifications and unresolved queries regarding the loan are common hallmarks of mortgage fraud.

Responsibilities of forensic accountants

Forensic accountants look at data to figure out where money has gone missing and how to get it back. They may also offer financial findings reports as evidence in court sessions, where they frequently testify as expert witnesses. Public accounting and consulting firms, law firms, law enforcement agencies, and insurance companies all benefit from this effort.

In each of these situations, the function of a forensic accountant differs. Each business handles money in a unique way, and con artists target businesses depending on their responsibilities. Some accountants, such as those employed by law enforcement organizations or law firms, work on larger fraud cases. Accountants in highly specialized industries, such as public accounting or insurance, usually concentrate on specific sorts of transactions.

Descriptive Analysis through case study

Case Study - 1

Investigating Embezzlement using Forensic Accounting

Culpepper CPA has been hired to look into a number of incidents involving "cooking the books" by a high-ranking executive or employee.

Uncovering clues is one of the most difficult aspects in situations of alleged theft, fraud, or embezzlement. When someone steals money, they try to hide their traces, and the more complex the fraud is, the more difficult it is to detect.

For example, they were once hired by a construction business to look into a CFO who was suspected of malfeasance. The company's owners accused the CFO of embezzling a large sum of money. Something wasn't adding up in the financials. The owners were aware of several suspicious transactions, but lacked the impartiality and training to connect the connection

They were able to sift through all of the bank documents, detail the numerous unlawful transactions, and provide conclusive evidence. The CFO had, in reality, manipulated payroll for the past three or four years to grant himself unauthorized incentives. Personal expenses were also charged to company credit cards, and personal bills were paid with company checks. Over $700,000 has been embezzled by the CFO!

They spoke with the CFO, who went on to become an ex-employee shortly after. They also collaborated with their client's attorney and insurance company to make a claim and obtain the

highest potential settlement. We testified as an expert witness when the corporation eventually chose to bring charges against the CFO.

Case Study - 2

Using Forensic Accounting to Prove Fraud

A school district was another of Culpepper CPA's customers. A principal was suspected of squandering school finances by many high-ranking administrators.

The principal paid $25,000 to $30,000 of his Master's degree tuition with school funding. He assisted his wife, a teacher at the school, in keeping a retired teacher, a personal friend, on the payroll. He also increased compensation or wages for employees who worked in before- and after-school programmes, even if they didn't work all of the days they were paid for. Some of them even took Paid Time Off (PTO) on the days that they were paid for after school! They were able to investigate these instances, record the multiple improper expenditures and fraudulent payroll, and provide the facts and context needed by the local board of education to fire the principal and initiate a counter-suit against the ex-principal.

Case Study- 3

Scam at Satyam Computers

This occurred between 2006 and 2008.Who were the participants: Rama Raju, B (Chairman, Satyam), Srinivas Vadlamani (Chief Financial Officer), T Srinivas and Subramani Gopalakrishnan (PWC Auditors, CFA)

Background:

The scandal was exposed in 2009, when Satyam Computers founder and chairman Ramalinga Raju admitted that the company's finances had been tampered with. In the balance sheets, he revealed a Rs.7,000 crore accounting scam. Ramalinga Raju acknowledged and confessed to inflating the company's cash and bank balances in an email addressed to Sebi and stock exchanges on January 7, 2009.

What occurred was this: Raju also tampered with the accounts by failing to include some revenues and payments, resulting in a Rs 12,318 crore misrepresentation, according to an examination of the data.

What action was done, and what was the outcome:

Following the discovery of the scam, the government authorized an auction to sell the firm in the best interests of investors and over 50,000 Satyam Computers workers. Tech Mahindra bought it, renamed it Mahindra Satyam, and later merged it with Tech Mahindra. According to Sebi's investigation at the time, the Satyam scandal finally turned out to be a case of financial misstatements of Rs 12,320 crore.

Case study - 4

The airline Kingfisher (KLA)

KLA was yet another corporate deception, the first of its type in the airline sector, that finally brought the King of Good Times' empire to an end. Vijay Mallya, well known as the "King of Good Times," founded the airline. KLA earned a reputation as the country's finest private airline in a short period of time, with a high grade of service and the second largest market share behind Jet Airways.

The corporation took up loans from all feasible sources, including related parties and a guarantee of the Kingfisher brand based on an overestimation of its worth. The good days didn't last long, and Vijay Malia was forced to sell his family's prized liquor and beer company to pay off some of his obligations. Vijay Malia is now in the United Kingdom, undertaking a legal struggle to prevent his return to India. A consortium of banks led by SBI has a Rs 9000 crore exposure to what is now a practically insolvent airline. The majority of employees were laid off or abandoned their employment since their salaries were not paid for months at a time. The corporation went as far as not submitting statutory dues to government agencies, such as PF and TDS deducted from salaries.

Case study - 5

Insurance fraud: 5 arrested on charges of fake life insurance claim in Telangana

In Telangana, five people have been detained on allegations of filing a false life insurance claim. They used to pick ill persons and those who were addicted to alcohol and persuade their family members to buy term insurance policies on their behalf.

They used to pick ill persons and those who were addicted to alcohol and persuade their family members to buy term insurance policies on their behalf. They used to pick ill persons and those who were addicted to alcohol and persuade their family members to buy term insurance policies on their behalf. Five scammers have been detained in Nalgonda district on suspicion of being involved in a scam.

Case study - 6

Cyber-crime: COVID-19 Results Database incident

An assault on government websites in early 2021 compromised a database containing the personal information of at least 1500 Indian residents. The data had been made publicly available via downloaded PDF files by the hackers. The attack was eventually discovered to have been carried out by New Delhi-based entities. A similar occurrence occurred in 2020, when a hacker gained access to the data of 80,000 COVID-19 patients from the Delhi State Health Mission database. The Kerala Cyber Hackers group claimed responsibility for the attack, claiming that it was motivated by anger with the government's treatment of healthcare workers.

Case study - 7

Ashok Iron Works Private Limited v. Karnataka Power Transmission Corporation (KPTC)

How did the case's factual matter come about?

The issue dates back to the turn of the century, when Ashok Iron Works, a private iron manufacturing firm, asked for electricity from the state's power generation corporation, the Karnataka Power Transmission Corporation (hereafter KTPC), in order to start producing iron. Despite paying costs and receiving confirmation for a 1500 KVA electricity supply in February

1991, the real supply did not commence until November 1991, 10 months later. The private corporation suffered damages as a result of the delay. This led a complaint under the Consumer Protection Act 1986 to the Belgaum Consumer Dispute Forum and then to the Karnataka High Court.

Case study - 8

The 2001 Stock Market Scam and Ketan Parekh

The year this occurred was 2001.Background: He had begun operating his family's brokerage firm as a chartered accountant via professional training. Ketan Parekh was acquainted with worldwide superstars like Kerry Packer during the height of his fame, and the two of them had co-founded a venture capital firm with the goal of investing in start-ups in India. What happened: From late 1998 to 2001, I was involved in an Indian stock market manipulation scheme. Ketan Parekh was on the lookout for stocks with a small market capitalization and little liquidity. He'd then invest money in these stocks and begin bogus trading inside his own network of businesses. On the bourses, the typical person may start.

Conclusion

Forensic accountants are experts in analyzing, interpreting, and summarizing complex financial and business issues. Insurance businesses, banks, police forces, government organizations, and public accounting firms may hire them. Forensic accountants gather financial evidence, create computer applications. Corporate fraud is defined as illegal, misleading behavior perpetrated by a firm or an individual who works for the company. Many corporate fraud schemes are complex accounting techniques that are used to exaggerate a company's apparent profitability and can take years to uncover. When large-scale corporate fraud is found, it has the potential to bring down even large multinational corporations with billions in yearly sales.to manage the data, and disseminate their conclusions through reports and presentations almost all bank fraud is a federal offense.

The Federal Deposit Insurance Corporation ("FDIC"), a federal agency that protects consumers' deposits in banks and other financial institutions, is responsible for most banks. Anyone who "knowingly executes, or attempts to execute, a scheme or artifice" to defraud a financial institution; or obtains any of the money, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises, faces a fine of up to $1,000,000, and may be imprisoned, according to FDIC laws and regulations regarding bank fraud punishment.

Insurance fraud occurs when either the buyer or the vendor of an insurance contract commits a criminal conduct. A seller might, for example, sell insurance from non-existent companies, fail to submit premiums, and churn policies to increase commissions. A buyer may also falsify medical records, exaggerate claims, fabricate death or kidnapping, and murder. The following steps can help to lessen cybercrime risks:

- Create cybersecurity incident response plans to complement these policies and processes; develop clear policies and procedures for the company and its personnel.
- A description of the security procedures in place to secure systems and company data;
- Apps that require two-factor authentication (2FA) or physical security keys should be used;
- When possible, enable two-factor authentication on all online accounts.

- Verify the legitimacy of money transfer requests by speaking with a financial management;
- Develop intrusion detection system (IDS) rules that flag emails with extensions that are similar to those used by your firm;

.

References

https://www.cyberralegalservices.com/casestudies.php
http://www.cyberlawclinic.org/casestudy.htm
https://www.investopedia.com/
https://scholar.google.com/
https://www.techtarget.com/searchsecurity/definition/cybercrime
https://www.justia.com/criminal/offenses/white-collar-crimes/bank-fraud/
https://jsberrylaw.com/blog/bank-fraud-definition-penalties/
https://corporatefinanceinstitute.com/resources/knowledge/accounting/forensic-accounting-litigation/
https://www.wirc-icai.org/images/material/Types-Fraud-Recognizing-Fraud-Indicators-KR.pdf
https://www.accounting.com/resources/forensic-accounting-basics/
https://us.aicpa.org/content/dam/aicpa/membership/downloadabledocuments/forensic-accounting-fraud-investigations-chapter1.pdf