Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Corporate Fraud: Data Theft and Misappropriation of Funds in India

Esha Gupta[a]

[a]NMIMS, Mumbai, India

Received 20 December 2022; *Accepted* 04 January 2023; *Published* 09 January 2023

Today, the focus of white-collar crimes has shifted from individuals to organisations, in which individuals alone or in partnership with others commit illegal acts. Corporate Fraud is one of thesewhite-collar crimes. Corporate fraud occurs when a firm or organisation alters or hides informationso that it seems to be in good financial standing. A firm may commit fraud by falsifying accounting records, concealing debt, or omitting to inform shareholders of executive loans and bonuses. The manipulation of financial information, such as fake accounting entries, fictitious trades intended to exaggerate profits or conceal losses, and phoney transactions, would assist the organisation in attracting cash from lenders and investors. There may be numerous reasons for a company to commit fraud, but the primary reason is to make money and create a false sense of financial stability for the firm in order to protect its reputation on the market and to mislead government agencies in order to avoid paying excessive taxes. This article illuminates the analysis of corporatefraud in India, focusing on data theft and misappropriation of funds.

Keywords: *data theft, corporate fraud, misappropriation of funds.*

INTRODUCTION

Corporate frauds are a kind of white-collar crime, not only happening in India but all across the world. White Collar Crimes are typically committed by society's elite as well as the most sophisticated members. They diminish interest and confidence in business investments, which in turn diminishes faith in government and society. Corporate frauds pose a higher threat to society than burglaries, robberies, etc., because the financial loss caused by corporate frauds is greater than that caused by burglaries, robberies, etc.

With the development of trade and technology, corporate fraud has become a global occurrence. India is similarly afflicted with corporate fraud as any other nation. This emerging nation's rapidly expanding economy and industrialization are to blame for the significant surge in corporate fraud over the past few decades.[1] In the broadest meaning, fraud is an intentional lie perpetrated for personal advantage or to harm another person or organisation. "Fraus Omnia Vitiate" means that fraud taints everything. Corporate fraud occurs when a company knowingly distributes false information intending to conceal the truth and fool the recipient of the data for financial gain.

Almost a third of Indian firms suffered thefts by both internal and external parties during the past year, with data theft being the most prevalent fraud incident, according to a survey published in 2019. According to Kroll's annual global fraud and risk study, 33% of Indian businesses suffered reputational loss at the hands of third parties, compared to 29% globally. In the past year, roughly 41% of Indian businesses were victims of data theft, although the global average was only 29%.[2] Data Theft refers to the unauthorised copying, removal, or theft of confidential or valuable information from a corporation, business, or individual without their knowledge or permission. In this theft, a person's password, personal information, banking, or financial information is at risk of being taken. Theft of sensitive information, such as customer data, software source code, company trade secrets, and confidential information, poses a threat to corporations and enterprises. The legal definition of Data Theft is provided in section 43 sub-clause (b) of the IT Act 2000, which states: If any

[1] Varsha Rajora, 'Corporate Frauds in the World of Corporate Sector: A Critical Analysis' (2010) SSRN E Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539013> accessed 02 October 2022

[2] 'One-Third of Indian Businesses Hit Hard by Internal, External Fraud: Report' (*The Economic Times*, 1 October 2019) <https://economictimes.indiatimes.com/news/company/corporate-trends/one-third-of-indian-businesses-hit-hard-by- internal-external-fraud-report/articleshow/71393811.cms?from=mdr> accessed 02 October 2022

person downloads, copies, or extracts any data, computer database, or information from a computer, computer system, or computer network without the permission of the owner or any other person in charge of the computer, computer system, or computer network. When information in the form of data is illegally duplicated or taken from a business or another individual without his knowledge or consent, this is referred to as data theft.[3]

According to a statement made by the company's board on March 2, Ashneer Grover and his familyhave been found guilty of misappropriating company cash, establishing a new front in the conflict between the two parties. It was also said that the Board is taking all necessary efforts to further strengthen the company's corporate governance, including the formation of an audit committee, an internal auditor, and the installation of other important internal controls.[4] According to the preceding statement, the accused was accused of misappropriating funds. The broad category of misuse of funds includes asset misappropriation, financial fraud statement, and stock fraud.

In the following paper, the notion of corporate fraud in India will be reviewed, followed by an analysis of the Companies Act of 2013. Data theft and misappropriation of funds will also be addressed, and the necessity for intervention will be emphasised in the context of corporate Indiatoday. The conclusion is then composed.

CONCEPT OF CORPORATE FRAUD IN INDIA

A firm or entity commits corporate fraud when it alters and hides important information in order to make itself appear healthy. Such corporate frauds are perpetrated by corporations using a variety of methods, including misrepresentation of information in the prospectus,

[3] 'Data Theft: Meaning, Laws Govern It, Liabilities of Corporate and Its Employees, Grievance RedressalMechanism and Penalties.' (*Legal Service India*) <https://www.legalserviceindia.com/legal/article-6734-data-theft-meaning-laws-govern-it-liabilities-of-corporate-and-its-employees-grievance-redressal-mechanism-and-penalties-.html> accessed 02 October 2022

[4] Priyanka Sahay, 'BharatPe board says Ashneer Grover and family misappropriated funds, reserves right to legal action' (*Moneycontrol*, 2 March 2022) <https://www.moneycontrol.com/news/business/startup/bharatpe-board-says-grover-family-misappropriated-company-funds-reserves-right-to-take-legal-action-8180671.html> accessed 02 October 2022

manipulation of accounting records, and concealment of debt, among others. The element of falsifying financial information encompasses fake accounting entries, false trades to inflate profits, the revelation of price-sensitive information that falls under the purview of insider trading, and the presentation of phony transactions that attract additional investors and lenders. Globally, corporate fraud scams have dominated the front pages of newspapers in recent years. From Enron to Satyam, there have been numerous high-profile incidents that have been extensively researched and discussed by professionals and subject matter experts. This issue's prominence is demonstrated by the fact thata Google search for "corporate fraud" returned more than 10 million results. Corporate scandals contributed to India's turmoil on the world stage. Below is addressed one of the most notorious cases:

Satyam Scam: The trial court found Ramalinga Raju guilty of the Satyam fraud and sentenced him to seven years of solitary confinement and a Rs. 5 million fine. The fraud shocked and scandalised the entire country. It is sometimes referred to as the Enron of India. One of India's major IT companies, Satyam Computer Services Limited (M/s SCSL), likely perpetrated the largest corporate fraud in history. Investors lost approximately Rs. 8,000 crores as a result of the fraud. Ramalinga Raju admitted in his letter that he falsified the company's books of accounts and that the accounting entries were inflated. In order to match the expectations of investors, he exaggerated the income nearly every quarter for several years. The fraud was also aided by incompetent independent directors and careless auditors.[5]

The Saradha Group Chit Funds scam: the Ponzi scheme was initiated by the issuance of redeemable bonds and secured debentures, together with the promise of irrationally high returns on reasonable investments, in order to collect funds from investors. Local agents were engaged throughout the state of West Bengal and offered enormous cash rewards from investor deposits inorder to expand rapidly, ultimately becoming a conglomerate of over 200 enterprises. The gang employed a network of firms to launder money in order to evade regulatory agencies. 15 million depositors and agents are estimated to have lost between $200 billion and $300 billion when the company failed in April 2013. The Securities and Exchange

[5] Shweta Wadhwani & Hema Menon B, 'Corporate Frauds: Emerging Issues and Preventive Strategies' (2020) 7(6) JETIR <https://www.jetir.org/papers/JETIR2006035.pdf> accessed 01 October 2022

Board of India (SEBI) prohibited Saradha Group and its managing director Sudipto Sen from participating in the securities market until the company terminates such programs and returns investor funds.[6]

CORPORATE FRAUDS UNDER COMPANIES ACT, 2013

The Companies Act of 2013 focuses on corporate fraud issues. Fraud in relation to the affairs of a company or corporate body, as defined by section 447[7] of the Companies Act 2013, includes any act, omission, concealment of any fact, or abuse of position committed by any person or any otherperson 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, regardless of whether there is any wrongful gain or wrongful loss. The new act includes a concept of fraud that is encompassing, but not exhaustive, and only applies to the affairs of a corporation or other legal entity. While the term fraud encompasses not only any 'doing,' but also 'the omission, not to act,' concealment of any fact, and abuse of position by a person.[8]These actions, omission, and concealment, can be committed by any individual on their own or with the aid of any other individual. For an act to constitute Fraud, it must be committed by a party to a contract with the intent to deceive another party or his agent or to convince him to enter into a contract. Fraud, which voids the contract, must have a connection to the parties' actions when they entered into the contract. This definition emphasizes the prerequisite for establishing the purpose of the perpetrator of the fraud. This individual will be punished if he has willingly committed fraud. This individual refers to him or his representative. The acts that constitute fraud are false assertions, concealment of facts, false promises, and any other fraudulent deception. The new law contains severe penalties for corporate fraud. Whoever is found guilty of fraud shall be punished with imprisonment for a minimum of six months, which may extend to ten years, and a fine corresponding to the amount involved in the fraud, which may extend to three

[6] *Ibid*
[7] Companies Act 2013, s 447
[8] Sanjeev Gupta, 'Corporate Frauds and their Prevention under the New Companies Act' (*ICAI*, May 2014) <http://drsanjeevgupta.net/wp-content/uploads/2019/12/corporate-frauds-and-their-prevention.pdf> accessed 01 October 2022

times the amount involved in the fraud. However,a minimum sentence of three years shall be imposed when the fraud affects the public interest.

DATA THEFT: ANALYSIS

Data theft, often known as information theft, is the unauthorised transfer or storage of private, confidential, or financial data. Typically, data theft occurs because the perpetrators wish to sell theinformation or use it for identity fraud. The data theft was originally largely a concern for businesses and organisations, but it is becoming an increasing concern for individuals. While the phrase refers to 'theft,' data theft does not actually include taking the victim's information or deleting it. Instead, when data is stolen, the perpetrator simply copies or replicates the data for their own benefit.[9] The IT Act of 2000 governs Data Theft in India extensively. Data Theft is defined and described in Section 43 of the Act, while Sections 65, 70, and 72 of the Act outline the penalties applied in theevent of Data Theft. In the instance of a Data Breach, several IPC sections may also be invoked. Sections such as 403 address the implementation of criminal penalties for the dishonest misuse or conversion of personal property for one's own use. Data is intangible, but if it is stored on a hardware drive, such as a floppy disc or a flash drive, and it is stolen, then section 378 can be called. In accordance with Section 63B of the Indian Copyright Act, anyone who knowingly uses a computer or a copy of a computer program that infringes on intellectual property is subject to prosecution. Courts have stated in decisions such as Govindan v Gopalakrishna[10] and McMillan v Suresh Chunder Deb and others[11] that a compilation formed by committing capital, time, talent, and effort, even if drawn from a common source, is a literary work and hence subject to copyright protection. The courts justified their rulings by arguing that even the smallest amount of originality in a compilation was protected and that no one had the right to appropriate the fruits of another's labour. Data theft is also addressed by the Credit Information Companies Regulation Act of 2005 (CICRA). In this act, standards are established for how an entity may acquire and keep an individual's data, and liability is imposed on the company in the event of

[9] 'What is data theft and how to prevent it' (*Kaspersky*) <https://www.kaspersky.co.in/resource-center/threats/data-theft> accessed 02 October 2022
[10] *Govindan v E.M. Gopalakrishna Kone and Anr* AIR (1955) Mad 391
[11] *Macmillan and Anr v Suresh Chunder Deb* (1890) ILR 17 Cal 951

a data breach or unauthorised modification.[12]

Liabilities on Employer: In accordance with Section 43A of the IT Act, a company is obligated to compensate the affected party if it negligently deals, handles, or processes personal or sensitive data on a computer system that it owns, controls, or operates, and that negligence resultsin a wrongful gain or loss to a third party. Before collecting any information, Rule 5 of the IT Rule2011 states that a corporation or a person representing a corporation must obtain the information provider's written agreement. Corporate or anyone acting on his behalf must not collect the information unless it is for a valid purpose and collection is required for that purpose. Corporate or anyone acting on their behalf who collects information directly from the information provider must inform the information provider of the following:

- That information is being obtained.
- The purpose for which the information is being collected.
- The information's intended receivers.
- The agency collects the information, including its name and address.
- The organisation was responsible for information retention.

The company should establish a Grievance Officer and publicise his name and contact information on its website. The Provider of the Information shall have the option of not supplying the information in the first place, as well as the ability to revoke their consent at any moment after providing it to the corporation or any individual representing the corporation.

Liabilities on Employee: Section 72A of the IT Act of 2000 made the employee accountable

[12] 'Data Theft: Meaning, Laws Govern It, Liabilities of Corporate and Its Employees, Grievance Redressal Mechanism and Penalties' (*Legal Service India*) <https://www.legalserviceindia.com/legal/article-6734-data-theft-meaning-laws-govern-it-liabilities-of-corporate-%20and-its-employees-grievance-redressal-mechanism-and-penalties-.html> accessed 02 October 2022

for the breach of data and disclosure that is likely to cause unjust gain or loss without the agreement of the individual. Rule 6(3) of the IT Rules 2011 stipulates that employees may also be held accountable if the sensitive information of the data provider is disclosed. However, the phrase "Consent" is not mentioned in this provision, making it unclear if liability will exist even ifsensitive information is released with consent.

MISAPPROPRIATION OF FUNDS: ANALYSIS

Officers and directors of a corporation are not permitted to knowingly and unlawfully use corporate cash for personal advantage or any other improper purpose. This type of misappropriation may even lead to criminal prosecution. Additionally, businesses are responsible for having internal measures to detect and prevent such thefts. Any false or misleading statements regarding misappropriation or the internal controls of a corporation may give rise to a securities fraud action. For instance, failure to disclose vulnerabilities in the company's internal controls or providing false assurances on the integrity of a company's internal controls can serve as the basis for a fraud claim. In addition, a corporation must include diverted monies in the officer's remuneration report. As a result, representations about the amount and type of remuneration are false and misleading if they fail to account for the diverted cash, and such false claims may give rise to a securities fraud lawsuit. Furthermore, when a corporation's executives misappropriate corporate funds, management's positive remarks about the company or its management's honesty or integrity may be misleading. These comments may also provide grounds for a securities fraud action.[13] Section 447 of the Companies Act, 2013 states that any person found guilty of fraud involving at least 10 lakh rupees or 1% of the company's turnover, whichever is lower, shall be punished with: Imprisonment for a term which shall not be less than 6 months but which may extend to 10 years; and a fine which shall not be less than the amount involved in the fraud, but may extend to three times the amount involved in the fraud. In accordance with the section's first exception, the minimum sentence of imprisonment cannot be less than three

[13] 'Misappropriation of Corporate Funds' (*Glancy Prongay & Murray* LLP, 25 February 2019) <https://www.glancylaw.com/practices/securities/common-types-of-securities-fraud/misappropriation-of-corporate-%20funds/> accessed 02 October 2022

years if the fraud in question affects the public interest. The second proviso to the section states that if the fraud involves less than 10 lakh rupees or 1% of the company's turnover, whichever is lower, and does not involve public interest, the maximum penalty that can be imposed on the person found guilty of such fraud is five years in prison or a fine of up to 50 lakh rupees, or both. The 2013 Firms Act gives the Serious Fraud Investigation Office (SFIO) the authority to investigate companies suspected of fraud. In addition, the Act grants the auditor the authority to denounce fraud to the central government. Also, section 36 of the 2013 Companies Act addresses the penalties for fraudulently enticing individuals to invest money. For the offence of money laundering, Section 4 of the 2002 Prevention of Money Laundering Act imposes a minimum of three years in jail and a maximum of seven years, as well as a fine.[14]

NEED FOR INTERVENTION

In response to the rise in corporate fraud, the Securities and Exchange Board of India (SEBI) has adopted numerous measures. It has taken measures to identify, reduce, or prevent fraud by intervening at various phases of the fraud's development. In addition, it has published a number of guidelines to combat systemic misuse. Having solid governance processes in place is a tried-and-true method for corporations to prevent malpractice. Corporate governance is a structure meant to ensure that the organisation is effectively managed. It consists of the board of directors, independent directors, and committees, such as the audit or ESG committees, tasked with reviewing the company's activities and ensuring its compliance with legal and regulatory standards. Corporate governance guarantees that a corporation operates for the benefit of all stakeholders, not simply the majority stockholders. In addition to providing strategic oversight, the system recognises possible dangers or early warning indications and takes prompt measures to reduce them.

CONCLUSION

Globally, and in India as well, corporate frauds are on the rise. Fraudsters view financial

[14] *Ibid*

institutions as a series of processes that they must conquer, but once they have, the rewards can beimmense. The system and society as a whole have been terrified by the enormous devil that is fraud. Corporate fraud has become a contentious issue for academicians, investigators, and expertswho study it, as well as for intelligentsia who debate it. Thus, society focuses more on dealing with the consequences of fraud than on avoiding it. In order to keep fraudsters away, legislators and regulators must go above and beyond. Though we have a variety of laws relating to corporate frauds, as mentioned previously, which can be used to investigate fraud-related cases, we can take strategic steps such as: Providing investigators and regulators, particularly SEBI, with more authority; implementing international financial reporting standards; and ensuring that enforcement agencies place a greater emphasis on the identification and prevention of such frauds, which is a major concern. Greater fraud reduction can be achieved by the punishment of corporate offenders and culpable parties. More focus should be placed on the implementation of the new regulatory paradigm; regulators such as SEBI, CBI, ED, and SFIO should maintain close communication; and the whistleblower policy is one of the most effective means of preventing corporate fraud.