Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Financial Frauds in India: An Analysis

Abhirami Balachandar[a]

[a]Symbiosis International University, Pune, India

Received 23 February 2023; *Accepted* 14 March 2023; *Published* 18 March 2023

This paper presents a comprehensive study of financial fraud in India. Fraud can be understood as planned criminal deception performed for personal gain and with the advancement of technology, financial frauds have reached a whole new range of deception and violation of privacy. The National Crime Records Bureau shows a drastic increase in cyber-attack in the digital banking domain. Various modes of financial fraud (offline/online) such as phishing, Identity theft, money laundering, siphoning, and so on have been explained in brief. The companies Act 2013 plays a vital role in curbing financial fraud through Serious Fraud Investigation Office, The National Financial Regulatory Authority, and Vigil Mechanism. The role and significance of other dominant legislations and regulatory bodies are also elucidated. Considerable efforts by the financial institutions are applauded but there is scope and necessity for better performance. A few fundamental and pragmatic suggestions are included. Cyber fraudsters' tactics for stealing sensitive financial information are complex and constantly evolving hence, financial institutions must rethink and realign their security procedures and risk tolerance.

Keywords: *fraud, crime, ncrb, company.*

INTRODUCTION

Fraud is as old as human civilization. The first recorded occurrence of financial fraud dates back to 300 BC, a shipping merchant from Greece, Hegestratos, fraudulently claimed insurance compensation after deliberately sinking an empty ship while the valuable cargo was safely

harbored elsewhere. To simply understand an act of financial fraud is the intentional misrepresentation or obfuscation of any information or material fact with an intent to deceive anyone for unlawful gain. Fraud can be inflicted against an individual, business corporation, or government agency and it often results in substantial financial loss. A scholarly definition of financial fraud can be summed up as, *'an uncommon, well-considered, imperceptibly concealed, time-evolving and often carefully organized crime which appears in many types and forms'*[1]. The offense of financial fraud has risen drastically in recent times. This trend is especially observed in the United States of America[2], the United Kingdom,[3] and the Netherlands[4]. The inclination of this upsetting behavior is because of the easy accessibility provided by cyberspace. The scenario in India is equally grim, more than 2.9 lakh cyber-attack in the digital banking domain have been recorded in the year 2020, which is 11.8% more than the previous year as per the data provided by the National Crime Records Bureau (NCRB)[5].

The RBI Master Circulars on Fraud stated that *'frauds are committed by unscrupulous borrowers by various methods including, inter alia, a fraudulent discount of instruments, fraudulent disposal of pledged /hypothecated stocks, fund diversion, criminal neglect and mala fide managerial failure on the part of borrowers. The Master Circular also refers to certain other methods, which include forged instruments, manipulated account books, fictitious accounts, unauthorized credit facilities, fraudulent foreign exchange transactions, exploitation of multiple banking arrangements, and deficiency on the part of third parties with a role in credit sanction/disbursement'*[6].

---

[1] Van Vlasselaer et al., 'APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions' (2015) 75 Decision Support Systems 38–48

[2] National Criminal Justice Reference Service, *Financial Crime Fact Sheet - Office for Victims of Crime* (Washingron DC) 2

[3] FIA, 'From Suspicion to Action' (*EUROPOL)* <https://www.europol.europa.eu/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf> accessed 5 December 2022

[4] StatLine Netherlands, 'Geregistreerde criminaliteit; regio (indeling 2013) 2005-2012' (*Open Data*, 2013) <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/80344NED/table> accessed 05 December 2022

[5] PTI, 'Over 290,000 cyber security incidents related to banking reported in 2020' (*Business Standard*, 4 February 2021) <https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html> accessed 05 December 2022

[6] Ministry of Finance, 'Comprehensive measures taken to curb incidence of frauds in Banks' (*PIB*, 27 July 2021) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1739661 > accessed 05 December 2022

According to credit agency TransUnion's latest quarterly research of worldwide online fraud statistics, instances of digital fraud have been growing since the start of the Covid-19 pandemic.[7]

TYPES OF FINANCIAL FRAUDS (ONLINE/OFFLINE)

Phishing[8]: It is the most common form of remote attack. Phishing involves the impersonation of a legitimate or reputable entity in an electronic conversation. The attackers make fraudulent attempts to seek sensitive information such as credit card numbers, passwords, or other credentials. Generally, an attacker sends an email pretending to be from a known enterprise such as a bank, to collect sensitive financial information.

Vishing[9]: Vishing or also known as voice phishing. This is similar to phishing. Here, the attacker uses the phone to reach the potential targets to obtain the victim's personal and restricted information. In vishing scams, a large number of attackers use cloned voice-banking systems that sound legitimate or identical to the original and authorized systems.

Investment frauds: This sort of scam may affect anyone with a rudimentary understanding of finance. Investors are deceived to invest in pseudo-business corporations. This is a typical method used by cyber fraudsters and it is conducted either online or over the phone. A 'pump-and-dump' tactic is also used, where someone calls another person claiming to have exclusive knowledge about a publicly traded firm that only he knows about. This encourages that person to invest in the company's shares because he or she anticipates a high and quick return. The offender 'dumps' his or her shares in the firm at the new high price to profit from the temporary increase. Following the failure of such a scam, the stock price drops, resulting in a profit for the fraudster at the expense of the duped consumers[10].

Money laundering: Money laundering is an illegal process through which the source of money is concealed and it is altered to make the source appear legitimate. Money laundering tagged

---

[7] *Ibid*
[8] T Brar et al., 'Vulnerabilities in e-banking: A study of various security aspects in e- banking' (2012) International Journal of Computing & Business Research
[9] *Ibid*
[10] A Beresford, *Securities/Investment Fraud* (Washington, DC: National White Collar Crime Centre Bryman, 2003)

with other criminal conduct has proved to be a deep-seated threat to the global banking system. The United Nation's record suggests that the illicit proceeds laundered per annum account for 2% to 5% of the global GDP or $1.6 or $4 trillion.[11] The recent BASEL AML Index for the year 2020 classifies South Asia as having the highest risk score and exceeding the global average across all categories. The report also highlights the reason for the poor performance, which includes poor quality of Anti Money Laundering and Combating Financing of Terrorism structure, corruption and bribery is at an all-time peak. It suggests that policymakers would need to take a systematic and comprehensive approach to reduce money laundering vulnerabilities and strengthen the financial and investment markets.

Computer viruses and Trojans: Viruses and Trojan horses are malicious applications that are installed without your knowledge on your computer. These applications may be designed to collect or harm information, slow down the computer's functionality, or bombard the user with advertisements. Viruses propagate by infiltrating and multiplying on computers. Trojans disguise themselves as legitimate software and then install themselves on a computer to observe and gather data. An apt example would be the love bug virus outbreak in the year 2000. LOVE-LETTER-FOR-YOU was the subject of an email attachment sent to victims. It was infected with malicious code that overwrote files, stole passwords, and sent copies of itself to all connections in the victim's Microsoft Outlook address book. The virus spread globally and infected more than 45 million computers. The cost of the virus attack was estimated to be around US $10 billion.

Skimming/ATM frauds: Card skimming is the unauthorized stealing of data from a credit or ATM card's magnetic strip. Scammers attempt to steal card information to gain entry into the user's account. Scammers can make a cloned card using the user's information after skimming the card. The scammer can then use the same account to rack up charges.

Identity Theft: Identity theft or identity fraud describes those crimes in which someone utilizes another person's personal information with the intent to deceive. It is usually performed for

[11] *Ibid*

financial benefit. In India, identity theft accounted for 77% of all fraud incidents in the first quarter of 2015. Credit cards have experienced the highest number of identity theft fraud instances, accounting for 85% of all reported frauds in the same quarter. The majority of identity theft takes place offline. According to McAfee, phishing scams and identity theft will continue to be a concern among consumers unless consumers are better educated and embrace preventive security.

Fraudulent Documentation: It is an act of editing, amending, or modifying a document to mislead another person. It can also entail intentionally endorsing inaccurate information in paperwork. Bank accounts with inadequate KYC procedures or inactive accounts are susceptible to fake documentation.

Siphoning: If money obtained from banks is used for activities irrelevant to the borrower's objectives, to the harm of the entity's or lenders' financial health. The lenders' judgment on whether a given incidence constitutes money siphoning would have to be based on verifiable data and details of the case.

REGULATORY MEASURES IN INDIA

Companies Act 2013[12]: This law contains several rules and protections for recognizing, preventing, and punishing corporate fraud. The Companies Act 2013 establishes the obligations of various persons/authorities/officials for fraud prevention and reporting, as well as giving a comprehensive understanding of the term, fraud. The Companies Act of 2013 emphasizes the fraud itself instead of the injury or damage to the concerned parties. The purpose or motive of the accused to perform such a fraudulent act is a critical component of the fraud offense.

Under Section 211 of the Companies Act 2013,[13] Serious Fraud Investigation Office (SFIO) can be established. It investigates and prosecutes white-collar crimes. The Companies Act also establishes the rights, responsibilities, and obligations of directors. There are also provisions in place to ensure that the business mechanism is transparent and that the decisions made are

[12] Companies Act 2013
[13] Companies Act 2013, s 211

answerable or justifiable. The National Financial Regulatory Authority (NFRA) is in charge of reviewing and enforcing compliance with the accounting and auditing criteria under this Act. It also provides for a 'Vigil Mechanism' it seeks to offer appropriate protection for workers and directors from being victimized[14]. When an auditor of a business has cause to suspect that an offense associated with fraud has been perpetrated against the company by officials or employees of the firm, the auditor must promptly disclose the same to the State authorities.[15]

Indian Penal Code 1860 (IPC): This legislation lays forth the penalties for the vast majority of criminal violations in India. The IPC inflicts a penalty on the following types of fraud:-

Criminal breach of trust[16]: Criminal breach of trust is characterized as dishonest misappropriation or taking over another's property for personal use in a deceitful manner.

Cheating[17]: This is done by anyone who deceives another individual, either fraudulently or deceitfully, into delivering or keeping the property.

Forgery[18]: This occurs when someone fabricates papers or e-data to inflict harm to the public or any individual, or conduct fraud.

The Competition Act 2002: The Competition Act makes it illegal to engage in anti-competitive conduct, such as exploiting a strong position in a given industry. It is also illegal for businesses to impose unfair and discriminatory conditions of sale, purchase, or service[19].

Right to Information Act 2005: RTI is a pioneering Act in India that attempts to increase transparency in government bodies. The Act was passed in 2005 as a result of anti-corruption campaigners' tireless work. It is referred to as revolutionary since it exposes government

[14] Companies Act 2013, s 177
[15] Companies Act 2013, s 143
[16] Indian Penal Code 1860, s 405
[17] Indian Penal Code 1860, s 415
[18] Indian Penal Code 1860, s 463
[19] Competition Act 2002, s 4

institutions to public criticism. A regular citizen can seek information from any government agency if he is familiar with RTI.

Prevention of Money Laundering Act, 2002[20]: India enforced the Prevention of Money Laundering Act 2002, in the year 2005. The banks are under an obligation to follow the guidelines issued by the Reserve Bank of India (RBI) based on the recommendations made by the Financial Action Task Force (FATF) and Basel Committee on Banking Supervision (BCBS) to curb money laundering activities and to combat the financing of terrorism. The Indian government also established, Financial Intelligence Unit (FIU-IND) in the year 2004. Its role of duties includes organizing and bolstering national and international intelligence, prosecution, and regulatory activities to curb money laundering and associated crimes. Enforcement Directorate (ED), SEBI, and RBI are other important agents of the Anti-Money Laundering unit in India.

Lokpal and Lokayuktas Act 2013[21]: The Lokpal (Central level body) and Lokayuktas (State level body) deal with Corruption charges and accusations of fraud against various government officials. These organizations serve as corruption ombudsmen, operating independently of the CGI's executive branch and state governments. These institutions have only recently begun to operate and perform in a limited capacity.

Securities Exchange Board of India Act 1992[22] (SEBI): SEBI controls the activities of the securities market, identifies fraud, and safeguards investors' rights. The SEBI is a statutory entity that works under the SEBI Act and is committed to addressing and prosecuting incidents of insider trading, market manipulation, and other financial crime. Special Courts of different jurisdictions within the country have been established to enable speedy and just trials of various financial crimes. SEBI can summon anybody involved in the securities market to appear in person, question them about their activity, and administer the man oath. Any individual familiar with the facts and details of the case may be summoned and compelled to give

[20] Prevention of Money Laundering Act 2002
[21] Lokpal and Lokayuktas Act 2013
[22] Securities Exchange Board of India Act 1992

testimony by the adjudicating official authorized by SEBI. Its regulations ensure that businesses and financial institutions follow the organization's objectives and standards of practice. The primary intention is to maintain the financial system efficiently. SEBI's developmental responsibilities include fostering algorithmic trading and updating economic structure. As an outcome of these initiatives, fraud and unfair behaviors are expected to be diminished. Its stated mission is to defend the interests of securities investors, promote the expansion and regulation of the securities market, and deal with issues that are related to or incidental to the securities market.

The Whistle Blowers Protection Act 2014[23]: The Whistle Blowers Protection Act of 2014 aims to provide a system for receiving complaints about corruption or intentional abuse of authority or judgment by public officials, investigating those allegations, and protecting complainants from persecution. Regardless of the widespread trend toward enacting higher barriers for whistleblowers based on national security concerns, nations such as India have experienced a rise in whistleblowing allegations, particularly those exposing corporate malfeasance.

Fugitive Economic Offenders Act 2018[24]: It was implemented to prevent economic criminals from avoiding the Indian legal system by avoiding the jurisdiction of Indian courts. The statute allows for the seizure of a fugitive economic offender's assets, confiscation of such assets, and the denial of the offender's means to defend any civil action.[25]

International Chamber of Commerce Rules (ICC Rules)[26]: In 1977, the International Chamber of Commerce issued its Rules of Conduct to Combat Bribery and Extortion. The 2011 ICC Rules include regulatory guidelines, which work towards ensuring anti-corruption rules are followed and preventive steps are taken.

Bank Case Information System (BCIS): To combat banking fraud, the Central Bureau of Investigation (CBI) has announced the development of a Bank Case Information System (BCIS).

[23] Whistle Blowers Protection Act 2014
[24] Fugitive Economic Offenders Act 2018
[25] *Ibid*
[26] International Chamber of Commerce Rules 1977

The names of accused people, debtors, and government workers have been gathered from previous entries in this database. The Reserve Bank of India (RBI) has unveiled a new structure to combat loan fraud, including leading indicators for banks and red flagging of accounts where defaulters will be denied future banking credit. It also intends to create a Central Fraud Registry that all Indian banks will be able to access. The CBI and the Central Economic Intelligence Bureau (CEIB) would also make their records available to banks.

SUGGESTIONS

- The very fundamental and easy-to-implement habit is to never share any sensitive or personal information with anyone. If such data is demeaned it is highly recommended to analyze the genuineness of the one asking for it.
- Antivirus software should be installed to protect the computer from harmful malware and viruses. Antivirus software should be updated regularly. Also, users must refrain from clicking on random hyperlinks from doubtful web pages or pop-up windows, or text messages.
- Due to the changing technological context, outdated methods of internal auditing must make way for new, technologically superior audit functions. Since fraud risk assessments necessitate considerable use of forensic and data analytics tools, flexible audit plans are essential.
- Establishing Multi Layered or Multi-Factor Authentication (MFA). It is a type of authentication that needs a user to give two or more confirmation criteria to obtain access to a resource like an app, an online account, or a VPN. A strong authentication and authorization policy must include multi-factor authentication. MFA needs one or more extra verification criteria in addition to a username and password, which reduces the chances of a successful cyber-attack.
- Officials particularly qualified to spot incipient scams must work for a specific fraud monitoring organization. Banks might also nominate one board member to be in charge of fraud risk management. Corporations must devote more attention to scams to increase the likelihood of early detection. This will also require improving their human resource

management practices and the capacity to pay the salaries required to hire fraud detection experts.

- There are decent legislations in place but the enforcement needs to be bolstered. As a consequence of poor financial literacy, there is a lack of information about financial products and their governance in smaller towns and villages, which leads to the growth of fraudulent transfers and Ponzi schemes.

CONCLUSION

In the globalized and board-less economic climate, India's financial sector is observing a dramatic increase in the domain of financial fraud. The progress made by the financial sector is appreciable but it comes with its drawbacks. Fraud causes enormous losses and projects a negative impact on service delivery. Apart from imparting financial literacy, and enforcing the updated legislation, financial institutions must work on strengthening their internal protection systems. Cyber fraudsters' tactics for stealing sensitive financial information are complex and constantly evolving hence, financial institutions must rethink and realign their security procedures and risk tolerance.