IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Cyber Fraud: Challenges for the Investors

Vishakha Bagdey
Assistant Professor
Late Govindrao Wanjari College of Law, Nagpur, India
vishakhabagdey@gmail.com

Abstract: *India is the fastest-growing country in terms of digitalization and technology. Investors are the pillars of the financial and securities market. When investors invest in the market, their money must be protected against losses that they are likely to suffer due to cyber fraud. The concept of investor considers several types of investors, who invested their money in in capital market bank or any other securities. Today people are aware of the importance and benefits of investment, so they invest in different investment options in various digital technology forms. Surly they are affected by the risk of cyber fraud. Nowadays cyber fraud is the biggest challenge for investors to tackle the complexity of the technological platforms and cyber issues. Not only India but Many countries face numerous security challenges, from financial fraud to data breaches and state-sponsored attacks, it can take various forms and the very sophisticated way it is increasingly. Focusing on this aspect researcher highlights the various aspects in this research paper. This current paper introduces the concept of cyber fraud in the financial sector. The Reasons Behind Cyber Attacks, what are the Challenges for the Investors? Also, mentioned are the Recent Cyber Fraud Cases and statistical reporting, Initiatives taken to curb Cyber Threats to Financial Systems, Compliance, and Regulation.*

Keywords: Cyber Fraud, Investors, SEBI, Statistic, Financial System, Legal Compliance

I. INTRODUCTION

In today's world companies operate their system through the Internet. Indian companies also run through the internet. India is the fastest-growing country in terms of digitalization and technology and one of the largest cyber hubs in the world. Even though having one of the world's fastest 5G rollouts, with 4.74 million base stations deployed, corporate investment in cybersecurity remains "minimal".[1] There is no doubt that cybersecurity and cybercrime are a worldwide burning topic right now. Which increased the risk of cyber threats and fraud.Many countries face numerous security challenges, from financial fraud to data breaches and state-sponsored attacks, it can take various forms and the very sophisticated way it is increasingly.

Fraud is a significant risk factor that can have catastrophic consequences for a company's finances. "Frauds can happen anywhere, whether it is the listed or unlisted space. It depends on the intention of the people," [2]There is no globally accepted definition of 'fraud.' Many countries' laws or statutes do not define it or specify the same.

According to English common law, "fraud" is dishonesty or deception. Any act, omission, or falsification of facts carried out with the intention of misleading, obtaining an unfair advantage, or harming the interests of a business, its creditors, shareholders, or any other individual is considered fraud. the crime of deceiving and fraudulently obtaining property delivery. It addresses fraudulent behaviors in which one person uses pretenses to trick another into giving up property or agreeing to its retention. According to RBI's guidelines on frauds, fraud is defined as "any intentional act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting in a wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."[3]Crimes performed by cybercriminals using the

[1] M U Nair, National Cyber Security Coordinator (NCSC).
[2] Sebi whole-time member S K Mohanty.
[3] Bharatiya Nyaya Sanhita (BNS) 318(4) is a section of Indian law addressing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

internet are collectively referred to as cyber fraud. The goal of these crimes is to unlawfully obtain and use private information belonging to a person or company to profit from it.

One type of cybercrime that uses deceit to steal money or private data is called cyber fraud. Incorporate:

• Hacking: Unauthorized access to data on a computer or network is known as criminal hacking.

• Malware. Any code intended to disrupt a computer's regular operation or perpetrate a cybercrime is called malware or malicious software.

Social engineeringidentity theft is two examples.

Piracy of software: Financial cybercrime covers things like identity fraud to apply for financial products, extortion, stealing payment card information, and gaining access to bank accounts to start illegal transactions.[4]

Reasons Behind the rise in cyber attacks

Rapid advancements in technology and digital transformation. Contactless payments, delivery apps, and remote jobs have all increased because of the COVID-19 pandemic.

Increased geopolitical tensions worldwide: For instance, a spike in cyberattacks following Russia's invasion of Ukraine.

Inadequate internal controls, Internal criminals were responsible for four out of ten platform scams in India. People are deterred from reporting these crimes by a lack of prompt action and detection.[5]

Key challenges for investors:

Investment platforms broadly are digital exchanges for investors to invest in stock markets across the world. Platforms using hard tokens and authentication where allow only a username, password, and to access the account. It is complicated for newly traded investors who are not generally 'tech-savvy.' The investors are not very much aware of their online security for the investment platforms they use. Investors have a limited understanding of the risks of using investment platforms.[6]Under the phishing scams, Fraudsters impersonate legitimate financial institutions through emails, SMS, or websites to trick investors into revealing sensitive login credentials and financial information.

Online platforms promoting fake investment opportunities with high returns, often with little to no transparency, targeting unsuspecting investors. Cybercriminals steal personal details to open fake accounts and conduct unauthorized transactions in an investor's name.

Malicious software that infiltrates devices to steal financial data or manipulate investment decisions.

Fraudulent cryptocurrency exchanges or investment schemes promise large returns with high risk.

Lack of awareness among investors regarding online security practices, making them vulnerable to scams

Difficulty navigating different regulations across various investment platforms, making it challenging to identify and report fraudulent activities

Tracing perpetrators across borders is complex, hindering investigations and recovery of stolen funds

Challenges in holding perpetrators accountable due to inadequate legal frameworks, slow investigation processes, and Limited enforcement mechanisms.lack of regulatory and supervisory frameworks and cyber-security workforce

Gaps in national and financial sector cyber-security strategies and coordination among stakeholders.

The Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and other authorities do not work together seamlessly, which results in a complex regulatory framework.

Legal framework issues: India, for example, does not have a specific legal system or court to address internet financial fraud.

[4] https://cybercrime.gov.in/webform/crimecatdes.aspx

[5] PwC's Global Economic Crime and Fraud Survey 2022

[6] Gerard Phillips, MSc (Royal Holloway, 2020) Geraint Price, ISG, Royal Holloway Online fraud and scams have dominated the cyber-enabled crime landscape.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

Recent Cyber Fraud Cases and Statistic Reporting

Two individuals were involved in a ₹8.14 crore stock trading scam. The victim reported being lured into a WhatsApp group focused on trading and investments. The scammers persuaded him to invest in block trades and Initial Public Offerings (IPOs) through a fraudulent application. Over three months, the victim transferred ₹8.14 crore into accounts linked to the scam.[7]Scams involving stock trading made up the greatest portion, with 2,28,094 complaints and losses of Rs 4,636 crore. Rs 1,616 crore was lost to "digital arrest" frauds across 63,481 complaints, while Rs 3,216 crore was lost to investment-based scams from 1,00,360 complaints.November 27, 2024. One of the cybercrime trends that is most seen as posing "high" or "very high" hazards worldwide is online scams. These days, digital services are essential to both public and daily life. As a result, more people—including those in vulnerable groups—are using the internet.[8]

Government data shows a massive surge in cybercrime incidents in India. Fraudsters cheated people out of Rs 33,165 crore in the last four years, including Rs 22,812 crore in 2024. Several Tier 2 and 3 cities were identified as cybercrime hotspots.

National Cyber Reporting Platform (NCRP), under the Ministry of Home Affairs, data shows fraudsters cheated people of Rs 551 crore in 2021, Rs 2,306 crore in 2022, and Rs 7,496 in 2023.

Data also shows that 1,37,254 complaints were received in 2021, 5,15,083 in 2022, 11,31,649 in 2023, and 17,10,505 complaints were received last year.The registry contains data of 1.4 million cybercriminals linked to financial fraud and various cybercrimes. [9]Maharashtra accounts for more than one-fourth of the amount lost due to cyber fraud in India

Moreover, the top 5 banks that suffered the highest share of fraud amounts are Kotak Mahindra Bank, Axis Bank, State Bank of India, HDFC Bank, and ICICI Bank. The order keeps changing, but they remained among the top five banks consistently across the five years of data used for this analysis. During these five years, these banks accounted for about 62% of the total value of reported fraud cases and about 53% of the total number of fraud cases. Of these five banks, the State Bank of India is the only public-sector bank. This shows that private sector banks are far more susceptible to cyber-attacks. Perhaps there may be a trade-off between being user-friendly and cybersecurity.[10]

It can cause irreversible and often irreparable damage to the image and reputation of a company. In recent times, with an increase in awareness, companies have started focusing on proactive risk management strategies in cybersecurity, which involve actively identifying potential threats, assessing vulnerabilities, and implementing preventive security controls to minimize the likelihood of cyberattacks before they occur, including practices like regular risk assessments, threat intelligence gathering, vulnerability scanning, security awareness training, and continuous monitoring of systems and networks.[11]

By releasing the Cybersecurity and Cyber Resilience Framework ("CSCRF") for SEBI Regulated Entities, the Securities and Exchange Board of India ("SEBI") made a significant contribution to enhancing the cybersecurity environment in India's financial sector.

In recent years, banks and other financial organizations around the world have faced a variety of cyber threats, from sophisticated and hazardous hacking on the financial markets to the theft of customer data. Thus, the CSCRF is an indicator of SEBI's strategy on how to address cyber risks and improve protection from cyber threats. The CSCRF is aimed to be comprehensive, spanning a spectrum of cybersecurity issues from preventive measures to response tactics.

To ensure that cyber security considerations are incorporated into all of the Regulated Entities' processes, SEBI requires that all Regulated Entities establish a dedicated cyber security committee under the CSCRF. This committee must include senior management and information technology specialists and be tasked with developing and monitoring the

[7] The Hindu Published - December 02, 2024, 07:05 pm IST - HYDERABAD

[8] INTERPOL Global Crime Trend Report 20222,

[9]https://indianexpress.com/article/india/cybercrime-sharp-rise-complaints-2024-govt-data-9816845/

[10]The Hindu November 13, 2024, 04:43 pm IST Md Zakaria Siddiqui,Sabir Ahamed

[11]Fraudulent Financial Practices and Investor Protection in The Indian Capital Market – Role of Sebi by Dr. Gaddam Naresh Reddy Principal Investigator Department of Commerce University College of Commerce & Business Management Osmania University Hyderabad 2018

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

implementation of cyber security policies. Protecting sensitive data is the most important part of the CSCRF. It requires that Regulated Entities implement robust data encryption, access controls, and privacy measures to safeguard sensitive information. This includes ensuring compliance with data protection regulations and maintaining transparency in data handling practices.

Furthermore, because cyber risks are constantly changing, the CSCRF must be updated frequently to handle all the new issues that arise. To keep the CSCRF current and useful, SEBI's dedication to ongoing development and interaction with the Regulated Entities will be essential.[12]

A third recommendation from SEBI alerted investors about unapproved platforms that sell fantasy games, paper trading, and virtual trading. To prevent fraud and financial losses, it advised investing only through licensed intermediaries. The advisory draws attention to the ways that specific web platforms and apps encourage paper trading, virtual trading, and fantasy games that are based on the stock prices of publicly traded businesses. SEBI explained that these actions are against laws designed to safeguard investors and that, to maintain safety and compliance, the public should only trade or invest through registered intermediaries.[13]

Initiatives taken to curb Cyber Threats to Financial Systems

The Financial Intelligence Unit-India (FIU-IND) oversees receiving, processing, evaluating, and sharing information about questionable financial transactions.

The Citizen Financial Cyber Frauds Reporting and Management System was created as a component of "The National Cybercrime Reporting Portal."

Computer Emergency Response Team-India (CERT-In): Gathers, examines, and distributes data about cyberattacks and sends out notifications

Chakshu: A campaign to enable people to report communications they believe to be fraudulent proactively

Better cyber-related governance structures at businesses and national cyber laws.

Businesses' insurance to guard against monetary damages from cyberattacks

Regular evaluation of the state of cyber-security and detection of possible systemic threats resulting from concentrations and interconnections, including those posed by third-party service providers.

The cyber risk may be decreased by promoting cyber "maturity" among financial sector companies, including board-level access to cyber-security knowledge that improves cyber-related governance.

Prioritization of data reporting and collection of cyber incidents, and sharing information among financial sector participants to enhance collective preparedness.[14]

Citizen Financial Cyber Fraud Reporting and Management System [CFCFRMS]

To promptly report financial cyber frauds and monetary losses resulting from the use of digital banking, credit/debit cards, payment intermediaries, UPI, etc., the Citizen Financial Cyber Frauds Reporting and Management System was created. [15]

Compliance and Regulation

Laws relating to Cyber in India play an important role in protecting the rights of individuals and organizations worldwide and ensuring a safe and reliable online environment.Information Technology (IT) Act, of 2000, and the Digital Personal Data Protection Act, of 2023. These laws cover cybercrimes, data protection, and cybersecurity.[16]Section 69 of the IT Act grants powers to the Central Government or its authorized agencies to

[12]Sanika Mehra is a Co-Managing Partner and Head- Corporate Practice and Antra Ahuja is a Senior Associate at Saga Legal.

[13]https://economictimes.indiatimes.com//markets/stocks/news/sebi-warns-investors-against-unauthorised-tradingplatforms/articleshow/114967913.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[14] https://visionias.in/current-affairs/monthly-magazine/2024-06-22/security/cyber-threats-and-financial-sectors

[15]https://i4c.mha.gov.in/ncrp.aspx

[16] Cyber laws justice Yatindra Singh Fourth Edition Universal Law Publication Company

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, February 2025

intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource in the interest of national security, public order, or for the investigation of a crime. India has made huge strides in cybersecurity by establishing the National Cyber Coordination Centre (NCSC) and the Indian Computer Emergency Response Team (CERT-In) to combat cyber threats, and data breaches and to improve cybersecurity resilience. The IT Act mandates companies and organizations to report data breaches within a 6-hour window of noticing such data breaches to CERT-In for investigation and response to cyber-attacks.[17]

In addition to implementing corporate-approved (board-approved) information security policies that effectively explain cybersecurity preparation, banks are required by the Reserve Bank of India Act of 2018 to develop and disclose their cyber crisis management plans. in situations where their cybersecurity standards are not being met. A fine of up to ₹10 lakh (₹1,000,000) may be imposed.

Authority for the Regulation and Development of Insurance (IRDAI). IRDAI regulates the insurance industry in India, providing information security requirements for insurers and stressing the value of data confidentiality and integrity.

Regulations pertaining to user data privacy and usage have been strengthened by the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI).

The Cyber Regulations Appellate Tribunal (CRAT) was established by the Central Government of India under Section 62 of the Information Technology Act, 2000, as the primary regulatory body and authority for gathering cyber evidence, interviewing witnesses, and determining facts..[18]

Suggestions

To address the intricate topic of financial cyber fraud and safeguard investor interests, a common, integrated platform must be established where all relevant parties, including banks, RBI, payment wallets, law enforcement agencies (LEAs), financial intermediaries, and the NPCI, collaborate to guarantee prompt and efficient fraud prevention measures.

Conduct Mandatory training sessions regarding the online complexity of the technology while entering the financial investment for the investors

India has legal frameworksabout cyber fraud, but there are slow investigation processes, Limited enforcement mechanisms,a lack of regulatory and supervisory frameworks, and a cyber-security workforce hence there is a need for a strong, efficient technology mechanism and cyber expert.

Remove the Gaps in national and financial sector cyber-security strategies and coordination among stakeholders.

The Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) are two regulators that must work closely together in the regulatory environment.

II. CONCLUSION

One significant risk factor that might have a catastrophic impact on a company's finances is fraud. It addresses fraudulent behaviors in which one person defrauds another by transferring property. An important step was taken by the Securities and Exchange Board of India to enhance cybersecurity in the country's financial industry. The most crucial way to guarantee safety and compliance is to protect sensitive data. By creating the Indian Computer Emergency Response Team and the National Cyber Coordination Centre, India has advanced cybersecurity significantly and strengthened cybersecurity resilience while thwarting cyberthreats and data breaches. Still, in India, four frauds in every ten platforms were conducted by internal offenders. Every Investment platformfor investors to invest in stock markets across the world is broadly in the digital exchange investment. It leads to a lack of internal control over them.As a result, online scams occur which pose ‘high’ or ‘very high’ cyber threats globally. India Government data shows a massive surge in cybercrime incidents in India. Every day huge complaints are registered by the investor's cyber fraud. Lack of regulatory mechanisms and Limited enforcement agencies unable to stop cyber-crime and cybercriminals. There is a significant need to tackle and punish the perpetrators.

[17] Cyber laws and Information Technology Dr. Jyoty Ratan 9th Edition 2022 Bharat Publication

[18] Cybersecurity Regulations in India: Kyle Chin updated Jan 02, 2025 https://www.upguard.com/