

Cyber Frauds and Banking Sector

V. K. Anand Krishnan and Meera Davi Chaliserry

*Assistant Professor, K J Somaiya Institute of Management,
Somaiya Vidyavihar University, Mumbai*

Email: anand.krishnanvk@somaiya.edu¹ and meera.chaliserry@somaiya.edu²

1. INTRODUCTION

With the rapid transformation of the financial landscape records the increase in the cyber frauds. The increase is further supported by the rising sophistication of the banking sector. Aslan, Aktug̃, Ozkan-Okay, Yilmaz, and Akin (2023) records a rise in the cyber fraud incidents from 5.3% in 2010-11 to 73.6% in 2021-22. Curtailing these cyber-crimes plays a significant role to prevent it from spiraling out to huge challenges.

The rapid advancements in digitalisation of financial systems have significantly affected the banking sector, with critical implications for emerging economies such as India. On the one hand, the development of mobile banking services, digital payment systems, and online financial services has enabled financial inclusion, reduced transaction costs, and improved efficiency. While on the other hand, these advances have significantly increased the vulnerabilities of financial systems to cybercrime. In this respect, cybercrime has become a key issue in the broader contexts of financial stability, risk, and regulation. Traditionally, cybercrime in the financial sector has been related to technological failures such as hacking, malware, and unauthorized access to financial systems. However, over the recent years, there has been a shift to behaviorally driven financial fraud. The modern nature of cybercrime involves the use of social engineering tools to exploit the psychology of the victims. This evolution of financial crime thus warrants a wider conceptualization of financial security to incorporate behavioural finance, information asymmetry, and bounded rationality.

The scale of cybercrimes in the banking sector has accordingly widened to include e-commerce fraud, investment scams, impersonation scams, and hybrid fraud structures. These frauds share common attributes of being highly flexible and having the ability to manipulate both technology and user behavior. However, of all these frauds, impersonation scams have proved to be highly effective due to their ability to create credibility and achieve compliance. A good example of this is the “digital arrest” scam, where fraudsters pose as law enforcement or regulatory authorities and coerce their targets into making payments. Contrary to other forms of cybercrime, these scams do not involve unauthorized

access of computer systems. Instead, these scams rely heavily on sustained psychological manipulation and perceived authority. This has also led to an understanding of how these frauds expose the limitations of conventional cybersecurity approaches that rely heavily on technological solutions. From an economic perspective, the implications of cybercrime are not limited to direct financial loss. The literature distinguishes between direct costs, such as unauthorized transactions, and indirect costs, such as reputational damage, operational disruption, legal liability, and loss of consumer trust. Recent literature suggests that in many instances, indirect costs are greater than direct costs, especially in the banking sector. A notable example is the case of State Bank of India (SBI). Given their systemic importance, any incident involving the bank tends to attract considerable media and public attention. It is noteworthy that in many instances of cyber fraud, especially those involving social engineering, there are no breaches of the system, as transactions are carried out through legitimate channels, albeit under false pretenses. However, these instances can lead to reputational damage, since customers are likely to associate the loss with the institution.

Finally, there are implications for financial markets and systemic risk. High levels of cybercrime risk can spill over into investor sentiment, affecting the valuation of financial institutions. This demonstrates the importance of considering cybercrime risk in the broader framework of financial risk management. Financial institutions and governments have responded to the development of cybercrime by employing multi-layered cybersecurity measures. Technological measures such as the AI-based detection mechanisms are at the heart of the development of cybersecurity measures. Simultaneously, institutional measures are also being implemented to enhance and equip organisations against a cyber-attack. This chapter examines the cybercrime in the context of the banking sector by combining theoretical discussions on the economic costs of cybercrime with emerging trends in cybercrime, its detection and prevention mechanisms.

2. TYPES OF CYBERCRIMES

Cybercrime in the banking sector consists of a variety of fraudulent activities, each of which takes advantage of specific technological loopholes of a firm or behavioral vulnerabilities of an individual. The classification of these crimes is of critical for understanding their mechanisms and for developing strategies for their prevention and detection. The next section describes the different categories of cybercrimes concerning the banking sector.

2.1 E-Commerce and Purchase Scams

These scams refer to the scams using the online marketplace and other electronic platforms to force the victims to purchase products that are never delivered. In such cases, the scammer usually advertises the products for sale at competitive prices and lures the

buyer into making advance payments. These cases are mostly reported for products that are in high-demand with low-value, such as smartphones and other electronic gadgets. Once the advance payment is made, the scammer goes out of contact with the buyer. These incidents are commonly reported during the period of high demand for such products. For instance, during major entertainment and sporting events, the scammer usually indulges in these scams by advertising tickets for these events on various electronic platforms and some social media sites as well.

2.2 Investment Scams

Investment scams refer to fraudulent investment schemes that lead people to invest in opportunities that are either non-existent or misrepresented intentionally. Some of the most common investment scams include:

- **Fake Deposit Schemes:** Fraudulent investment opportunities disguised as bonds or long-term deposits in reputed firms.
- **Boiler Room Scams:** Use high-pressure sales techniques to induce people to buy stocks at inflated prices
- **Fraudulent Cryptocurrency Investment Schemes:** Scammers use fake digital currencies or applications to induce people to invest in funds, leading to financial loss.

2.3 Impersonation Scams

Impersonation scams are those in which the scammer poses as a trusted figure to deceive the victim into revealing sensitive information or sending money. These scams are becoming more sophisticated, with scammers using digital communication, including emails, phone calls, social media, etc. The scammers use genuine documents, as well as email IDs that are very similar to genuine ones, to deceive the victims. Some of the popular impersonation scams are as follows:

- **CEO Scam:** In this type of scam, the scammer poses as the CEO of the organization and instructs the employees, customers, as well as vendors, to transfer money.
- **Bank Employees:** This is another common type of impersonation scam in which the scammer tricks the victim into sending money to the accounts they manage.
- **Impersonating Authorities:** In this type of scam, the scammer poses as a government official, as well as law enforcement personnel, and in some cases, they even put the victim in cyber arrest, preventing them from reaching out to anybody.
- **Financial Advisors:** In this type of impersonation scam, the scammer poses as financial advisors, including accountants, to deceive the victims with financial advice.

2.4 Romance Scams

These are cases of fraud in which scammers use dating sites, social media sites, and messaging apps, to create false profiles with the aim of establishing deceitful romantic

relationships with potential victims. In this type of scam, the scammers use images taken from other people, as well as false personal details, to create believable internet profiles, mostly for people living in a location different from the victim's location. Once the relationship is established, the scammers request money from the victim on the pretext of medical, financial, or travel issues aimed at visiting the victim. In addition to the financial loss, the victim in this case is likely to suffer from the emotional impact, as the scammer may have betrayed the trust of the victim in a romantic relationship.

2.5 Advance Fee and Payment Scams

These are the types of fraud schemes in which the victims are tricked into paying in advance for certain products or opportunities that do not exist. In this type of fraud, the fraudsters may promise the victims certain benefits in exchange for an upfront payment or certain personal information.

2.6 Business Email Compromise

Business Email Compromise is a type of cyber-enabled fraud in which the fraudsters gain access to or pose as legitimate business email accounts for the purpose of making unauthorised financial transactions. This type of fraud is usually carried out through cyber intrusions that allow the fraudsters to manipulate email communications within or across organisations.

2.7 Hybrid and Blended Scams

Hybrid or blended scams refer to those types of fraud schemes that combine aspects of two or more types of fraud schemes. This makes them complex and harder for the victims to identify. This type of fraud allows the fraudsters to exploit their victims for longer periods. One example is the recovery scam, which specifically targets the victims, who have already lost a large amount. In this type of fraud, recovery firms trick the victims into thinking that they can recover the lost funds.

3. ECONOMIC COST OF CYBERCRIME

The recent literature (Akinbowale, Klingelhofer, & Zerihun, 2020) in cybercrime domain attempts to assess the economic cost that a firm incurs after a cybercrime attack. This is important in analysing the impact of cybercrime and formulating a proper regulatory compliance strategy. In one of the pioneering studies in this domain, Anderson et al. (2013) proposes a systematic framework for the analysis of the economic impact of a cybercrime. The framework classifies the financial impact of cybercrimes into three dimensions: direct financial loss, indirect costs, and defence costs. While the direct financial loss comprises the immediate financial loss faced by the firm as a result of the cybercrime, the indirect costs include the contingent financial impacts of cybercrime, which are typically intangible in nature, such as financial loss arising from business disruptions, damage to

the firm's reputation, or the loss of intellectual property. Defence costs, on the other hand, include the investment in the firm's cybersecurity so that the firm is in a better position to defend itself against future cyber-attacks. These costs typically involve investment in new technologies, new software, new antivirus, or even hiring an in-house cybersecurity team. Interestingly, as Anderson *et al.* (2013) points out, in most of the cases, the indirect costs far exceed the direct financial loss as well as the defence costs, thereby underscoring the fact that the financial impact of cybercrime far exceeds the immediate financial loss.

Direct costs form one of the major and easily identifiable areas of the financial losses incurred by the firm. These financial losses are usually the result of direct theft or unauthorized financial transactions. There are several schemes that cybercriminals engage in for extracting the amount. These include phishing emails and schemes, as well as ransomware schemes. The financial losses are then incurred by the victimized firm. Cobos, Cakir, Straub, Qiang, and Torgusson (2024) suggests that direct costs are tangible and easily quantifiable compared to other types of financial losses. However, Cobos *et al.* (2024) also suggests that direct financial losses do not give an accurate picture of the impact of cybercrime because they do not consider the contingent impact of cybercrimes. In general, the indirect costs of cybercrime include financial costs due to reputational damage, business disruptions and legal penalties. When a firm is under attack, the overall business operations are affected due to system failures or network shutdowns. This may lead to productivity loss, which in turn may affect the overall operations and revenue. A good example is a ransom attack that may cause the business to shut down or cease operations until further notice. According to the literature, this may cause a financial cost to the business even if the amount lost in theft is minimal.

Another significant cost associated with cybercrime is reputational damage. The impact of cybercrime on business reputation is not discussed sufficiently in the literature. Trust is one of the most critical factors considered while conducting any business, especially in industries such as banking, where huge amounts of sensitive customer transaction data are processed. Studies have shown that companies that have faced cybercrimes and data breaches may face reputational damage, as customers may not trust companies that have failed to secure their sensitive data, resulting in high client turnover (Ali, Ali, Surendran, & Thomas, 2017). In addition, (Arcuri, Brogi, Gandolfi, *et al.*, 2017) the impact of cybercrime on the stock price performance of the targeted firm, suggesting that cybercrime is followed by a decline in the stock price performance of the targeted firm, as shareholders express their concern about future liabilities that may result due to cyber breaches.

Another particularly important category of cybercrimes that a firm may incur is the theft of the firm's intellectual property. These include financial costs associated with the attacks on the firm's proprietary technologies and other sensitive information. (Lewis & Baker, 2013) indicates that the financial costs of these crimes can be very severe, particularly in an industry like the AI or IT sector, where innovation and intellectual property constitute the competitive advantage of the firm.

Another indirect cost of the firm is the financial costs associated with the legal and regulatory repercussions of the attack. The data protection regulations in the world have become very strict, and this has worsened the financial costs associated with the attacks on the firm's cybersecurity. The victimised firm may be forced to pay huge fines and compensation to the affected customers. Industrial reports¹¹ on the financial costs of the attacks indicate that the attacks impose huge costs on the firm in the post-attack period. Thus, the attacks not only disrupt the normal business of the firm but also expose it to legal liabilities and compliance costs.

The banking sector is one of the areas that have received a great deal of attention in cybercrime literature, especially considering the level of exposure of the industry to digital transactions. Njeru and Gaitho (2019) claims that, considering the emergence of technology and the fact that financial transactions are being conducted online, banks are at a greater risk of being affected by cybercrime, especially cyber fraud, phishing, and unauthorised access of financial data. While many studies provide an in-depth discussion of the financial impact of cybercrime, (Bernik, 2014) argue that the economic impact of cybercrime is exaggerated. According to Bernik (2014), the cost of running a company also includes the cost of measures aimed at preventing cybercrime. This also underscores the importance of understanding the different types of cybercrime cost.

Although it points out that there is a need to isolate the real economic impact of cybercrime, challenges in measuring costs remain a recurring theme in the literature (Anderson *et al.*, 2013). Some studies point out challenges in accurately estimating the economic cost of cybercrime due to inefficiencies in data availability and methodological inefficiencies. Moreover, there are instances where victim companies do not reveal the real impact of cybercrime due to regulatory concerns. Lack of a concrete reporting structure also makes it difficult to estimate the cost of cybercrimes, as the available dataset lacks sufficient information due to underreporting. Although cybercrimes are common in every economy, according to the Armin, Thompson, and Kijewski (2016), it is difficult to compare studies due to a lack of standardised definitions and metrics, as well as a lack of clarity regarding reporting frameworks. On a similar note, studies such as the Riek and Bo'hme (2018) point out that cybercrime costs tend to be extremely skewed, such that a small number of cybercrimes results in a significantly high loss. In this context, the focus of the research in the future should be on the development of standardised measurement approaches and concrete frameworks for ensuring transparency in the reporting of cybercrime incidents, as well as more robust and diversified research studies at the firm level to understand the overall impact of cybercrimes.

4. DETECTION OF CYBERCRIMES

The banking sector employs a wide range of complex detection systems to combat the rising threat of cybercrime and financial fraud in the financial system. With the growing

1. <https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---the-economic-cost-of-cybercrime.pdf>

age of digital financial services, institutions are obliged to put in place complex detection systems that combine technology, as well as institutional processes. Additionally, some of the detection systems commonly used by the financial sector also include the use of real-time transaction monitoring systems.

These systems monitor different parameters such as the transaction amount, transaction frequency, geographical location, device identification, and the transactional history of the customer. Once such irregularities are detected, alerts are triggered to prevent such transactions. Apart from using such rule-based monitoring systems, banks are increasingly using advanced data analysis tools such as artificial intelligence in the detection of fraud transactions.

Machine learning algorithms allow financial institutions to process large amounts of transactional data and identify different patterns in the transactions. These patterns are often difficult to identify using traditional rule-based monitoring. Machine learning algorithms are continually learning from the transactional data and are thus increasing their ability to predict and identify different patterns in transactions. Another important tool in the detection of cyber threats is behavioural analytics, which is focused on monitoring the customer behaviour.

Banks make use of various parameters to generate the behavioral profile of the customers, such as login time, device type, transaction timing, and expenditure patterns. Significant variations from the established behaviour patterns may also set off alarms and necessitate additional verification measures. Behavioural biometrics such as keystroke analysis, mouse dynamics, and touch-screen analysis also help in the detection of fraudulent activities by identifying the fine differences between the real customers and the potential fraudsters. Besides transaction monitoring and behavioural analysis, banks are also increasingly using device monitoring and network monitoring tools to identify unauthorised access attempts and cybercrimes by monitoring the device types, IP addresses, browser fingerprints, and network geolocation of the customers.

Furthermore, if the login attempt is made from an unfamiliar device or from a high-risk region, additional measures of verifying the customers are also undertaken by the system itself. Network analytics and link analysis tools help in the identification of organised cybercrime activities by analysing the relationship between accounts, transactions, and digital identities to identify the underlying relationships that are otherwise not apparent on the surface. Furthermore, biometric-based modalities such as fingerprint scanning, face recognition, and voice recognition are also being integrated with digital banking systems to provide an additional layer of fraud detection and prevention mechanisms to the banks to ensure that access to the accounts is granted only to the real individuals and not the would-be identity thieves or takeover fraudsters. Another significant aspect of detecting cybercrime within the banking sector is the usage of forensic accounting and digital forensic investigation methodologies.

Once the patterns of suspicious transactions are recognised as indicative of fraudulent activity, the transactions are examined by specialised investigative teams to identify the sources of fraudulent transactions. These processes not only help in resolving cases of financial fraud but also strengthen the framework of institutional financial fraud detection by highlighting the weaknesses of the system. Financial institutions are also using cyber threat intelligence systems to collect and process information related to emerging threats of cybercrime, such as different forms of malware, phishing attacks, and other forms of cybercrime. Jointly working with the relevant bodies and other financial institutions can help disseminate information regarding emerging threats of cybercrime, which can strengthen the financial sector against cybercrimes.

5. PREVENTION OF CYBERCRIMES

The halting and identification of fraudulent practices hamper the functioning of financial institutions. Enforcing regulations, policies, and security mechanisms helps the banking sector navigate a challenging environment. Increased digital bank services, along with easier and broader access to financial services through digital penetration, have also led to a proliferation of cybercrimes. Effective fraud detection measures are essential to safeguard financial transactions and limit the impact of these crimes on all stakeholders.

Financial transactions must be regularly examined to detect fraudulent activities. Some common practises for these include early warning systems and AI-powered solutions. Along with the new-age measures, the banking sector continues to educate customers at various levels. They regularly send messages to their customers, organise structured sessions, distribute pamphlets, create engaging short videos, and take other traditional measures. Thus, with a combination of new-age measures and traditional approaches, financial institutions adopt measures to reduce digital fraud (Prashanth *et al.*, 2026). Automating fraud prevention methods brings with it a plethora of opportunities and challenges. Building customer trust while handling sensitive information with the utmost priority. Financial organisations also attempt to flag suspicious transactions using fraud detection systems (Kannan & Somasundaram, 2017).

The KPMG Global Scam Survey, 2025², identifies some of the most widely accepted preventive measures worldwide. The study highlights that, among all the measures adopted, blocking or pausing transactions by banks that seem suspicious was rated highly efficient (91% of respondents). Another measure that gained traction was either freezing the account or contacting the customer, and the measure that received the fewest votes was confirmation from the payee and customer education. The study notes that obtaining confirmation from the payee would only confirm that the credentials provided matched the financial institution's records, which might not reduce planned fraud. Likewise, they explain the possibility that customers may forget the various educational

2. <https://assets.kpmg.com/content/dam/kpmgsites/au/pdf/2025/kpmg-global-banking-scam-survey-2025.pdf>

measures adopted by banks. Some of the other measures are directed towards evaluating the vulnerable customers and monitoring their transactions, creating limits on their transaction amounts, adopting additional approval mechanisms, etc.

Adoption of the fraud detection mechanisms has multiple implications for financial organisations and for the stakeholders at large. (Bruno, Pistoletti, & Teti, 2025) link the role of cybersecurity and sustainability through the channel of financial stability. They also elaborate on the findings through the institutional and stakeholder theories and emphasise that prevention mechanisms help in shaping bank profitability and sustainability. Prior research highlights the implications of a breach of security in the financial aspect, leading to reputational and financial loss. The findings draw attention to the fact that improving the focus of financial institutions on the aspects of security and cyber fraud leads to improved reputation, thereby improving the image and trust customers and the stakeholders have in these institutions. Walter (2013), Walter (2016) and Willison and Warkentin (2013) elaborate that the role of reputational management for financial institutions is critical in situations of financial crisis and heightened customer expectations in terms of sustainability.

Engaging in sustainable measures results in improving corporate reputation and risk management; however, its impact on the profitability of the bank is debatable. Financial institutions also must balance between financial stability while keeping value creation through sustainable objectives; at the same time, manage the regulatory framework. Financial institutions, while adapting to the digital innovations, need to ensure data privacy, ethics and accessibility (Najaf, Mostafiz, & Najaf, 2021). Reducing the possible cybersecurity breaches, assuring regulatory compliance and reducing data privacy enhances the financial stability and the overall corporate sustainability (Karagozoglu, 2021). They also suggest that firms which combine digital transformation and new-age technology would be able to perform better than firms that would take a conservative stance. Xu (2024) also emphasises that banks improving through digital transformation, innovation and adopting measures to prevent cyber-crimes can mitigate the cost of operational risks. The transformation adds to the competitiveness of the financial institutions. Bruno *et al.* (2025) thus illustrate financial institutions should have a balanced approach while incorporating ESG to aid the financial reputation and image. The findings of Al-Alawi and Al-Bassam (2020) and Kwilinski, Lyulyov, and Pimonenko (2023) corroborate the positive association of engaging in cybersecurity and ESG. The regulatory bodies and the financial institutions individually engage actively in increasing the knowledge of the customers and all the stakeholders about cybercrimes and how to prevent them. To engage with the stakeholders, the financial institutions issue pamphlets, structured lectures, and short videos with animations which aid stakeholder knowledge of the possible fraud.

Another measure in which financial institutions engage is the Zero Trust Architecture (ZTA). A concept which explains “never trust, always verify”. This measure, by default, does not trust any user, system or device outside or inside the financial institution ecosystem.

The banking sector's application and net banking services request verification passwords and one-time passwords to ensure efficient verification. The core concept of ZTA is to verify every time an attempt to access the facility of the financial institution. Presently, the banking sector engages in integrating AI to reduce the possible cybercrimes. Through real-time fraud detection, AI Agents try to delay the outgoing payments in case of high-risk transactions. Banking sectors presently replace the traditional measures with AI models to identify anomalies. Further, AI integrated multi-layer security protocols enables to identify risk transactions. Thus, AI is utilised to ensure financial institutions move ahead of cyber criminals and the possible cyber threats.

One of the significant advantages that blockchain technology offers is the immutability of transactions. When a transaction is validated and included in the blockchain, it cannot be changed or deleted without the approval of the network's participants. Each transaction is secured through cryptographic hash and signature, and therefore, the financial data remains unalterable. This immutable system enables banks, auditors, and regulators to track suspicious transactions and detect fraudulent transactions in real-time. Utilizing blockchain technology in the financial sector aids transparency and improves the accountability in the bank transactions (Chhabra Roy & Prabhakaran, 2025).

Despite all these measures adopted by the financial institutions and the various stringent regulatory measures enforced by the regulatory organisations, the pandemic period witnessed the rise in cybercrime³. The growing reliance on online platforms for e-payments has opened new avenues for cybercriminals to intensify their fraudulent operations (Ma & McKinnon, 2022; Naidoo, 2020). Further, drawing attention towards how to decrease the cyber-crimes prevailing in society. Research throws light on how financial literacy aids the detection of fraud attempts. Lusardi and Mitchell (2014) has also elaborated how financial literacy impacts the economic behaviour and financial decision making.

Increase financial literacy improves better wealth accumulation at a granular level Stango and Zinman (2009) leads to rising participation in capital markets and debt management (Lusardi & Mitchell, 2014) and higher income (Stella, Filotto, & Cervellati, 2021). Isaia, Oggero, and Sandretto (2024) also illustrate how financial literacy acts as a mediator in reducing the financial frauds. Their findings also elaborate on the pivotal role financial literacy has in reducing the possible financial frauds the employees who engage in remote working face. Lusardi and Mitchell (2014) also emphasise that individuals who have higher financial literacy are able to detect the financial frauds initially. Further customers who are higher on financial literacy tend to adopt better security mechanisms while availing the banking services. Singh and Misra (2023) also reinforce that individuals with lesser financial literacy are prone to various scams and fraudulent operations.

While banks and other financial institutions across the globe are using several fraud prevention mechanisms such as artificial intelligence, biometrics, blockchain,

3. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>

and regulatory compliance, the effective implementation of these fraud prevention mechanisms is a complex challenge. The challenges include technological changes, regulatory compliance, and operational limitations. These are the key challenges that need to be considered for effective fraud prevention mechanisms within the banking industry.

One of the main challenges that are faced in implementing fraud prevention technologies is the complexity involved in integrating sophisticated technologies with the traditional banking system. It is found that traditional banks are still using legacy technology, which was developed prior to the emergence of digital banking and real-time transactions. The legacy technology lacks compatibility with sophisticated fraud detection technologies like machine learning, big data, and cloud-based technologies. It is found that integrating sophisticated fraud detection technologies with traditional banking systems is technically challenging.

Another challenge that is faced in implementing technological solutions in fraud detection is the complexity involved in integrating multiple data sources. It is found that fraud detection technologies need access to multiple data sources, such as data related to online transactions, mobile transactions, credit cards, and payment gateways. However, banks face difficulties in integrating multiple data sources, which affects the efficiency of fraud detection technologies in identifying fraudulent transactions. Studies on fraud management in banks reveal that difficulties in data integration and lack of technological tools are some of the key factors that reduce the efficiency of fraud detection technologies in traditional banks. Moreover, real-time monitoring systems require considerable computational power to process a large number of transactions in real-time. With the rise in the use of digital payments, the volume of financial transactions that need to be processed by financial institutions such as banks has also increased. If fraud detection systems are unable to process financial transactions in real-time, fraud may occur, and financial losses may be suffered before such fraud is detected.

Despite the many technological and regulatory mechanisms that banking sector have developed to curb cyber fraud, there remain several challenges that have hindered the successful implementation of the mechanisms. These challenges include the difficulties that financial institutions face while trying to integrate these technologies, the high cost of implementing the technologies, the challenges that banks face from cyber threats, the regulations that banks have to comply with, and the inefficiencies that banks face. Most banks continue to use the traditional banking systems that were not designed to counter the cyber threats that the banks face. Therefore, even if the banks manage to acquire the latest technologies, including AI, real-time monitoring technologies, and blockchain technologies, the effectiveness of the technologies may be compromised due to the traditional banking systems. In addition, the high cost involved in the implementation of sophisticated fraud detection technologies may serve as a hindrance, especially for smaller financial institutions that may not have the financial capability to invest in sophisticated cybersecurity solutions. The implementation of continuous monitoring solutions, data analytics solutions, and secure authentication solutions may require substantial financial

investments. Additionally, the fraud prevention solutions need to be upgraded constantly to respond to the changing tactics of cybercriminals. The fraudsters are constantly developing new techniques such as phishing, social engineering attacks, and malware attacks to take advantage of the weaknesses in digital banking systems.

These issues are to be addressed through collaborative efforts of financial institutions, regulatory bodies, technology developers, and customers themselves. First, financial institutions must invest in new technological advancements to build robust systems to deal with fraud detection issues. Moreover, financial regulatory bodies must formulate frameworks that are highly adaptable to changing financial technologies. This will enable them to respond to new technological advancements in a timely manner. On the other hand, banks, technology developers, and cybersecurity experts can collaborate to develop more advanced systems to detect fraudulent activities in real time.

Moreover, the development of a workforce with robust skills in cybersecurity is vital in the development of robust fraud prevention mechanisms. This is because the workforce is needed not only to develop robust security technologies but also to respond adequately to security threats. Additionally, enhancing customer awareness is vital in the development of robust fraud prevention mechanisms. This is because the more aware the customers are, the less likely they are to fall prey to cybercrimes. Therefore, with continued investment in technology and human capital, the stability of the global banking industry will be ensured in the long term.

6. DIGITAL ARREST FRAUD: THE CASE OF SBI

Online banking systems and digital payments have significantly increased financial inclusion and transactional efficiency in the Indian financial system. However, it is also notable that this technological infrastructure that supports a digitalised financial system has also created vulnerabilities in recent years. Some of the most alarming cyber scams that have come into existence in recent years include the “digital arrest” scam. In this type of cybercrime, scammers use psychological manipulation instead of exploiting technical vulnerabilities in systems and target bank account holders by assuming the role of law enforcement agencies and forcing them to conduct financial transactions. Some such cases have been observed in bank accounts operated by major financial institutions such as the State Bank of India (SBI).

6.1 The Nature of the Digital Arrest Scam

The modus operandi of a digital arrest scam usually begins with a phone or video call in which the scammers pose as officials from various law and order organisations, including the police, the Central Bureau of Investigation (CBI), and other government departments. The victim is misled into believing that their identity, bank account, or mobile phone is associated with illegal activities like money laundering and drug trafficking. The scammers then convince the victim that they must undergo a “digital arrest” and have

to remain connected through a video call at all times until the investigation is over. The victim is intimidated with the fear of legal consequences and is forced to send money to accounts claimed to be for “verification” and “temporary holding.” In reality, the money is sent to a pool of fraudulent accounts controlled by the scammers. What makes the process different from other cybercrimes is the amount of psychological manipulation involved in the scam. The scammers keep the victim connected through a video call for a very long time, sometimes even days, and ask them not to mingle with other people.

They even produce fake documents like arrest warrants, identity cards, and court notices.

6.2 Incidents Relating to SBI Customers

Recent cases reported in India show that the procedure involves the victim sending money to the cybercriminals. For instance, a retired bank employee in Navi Mumbai lost around 26.4 lakhs after the scammer, claiming to be an official with the National Investigation Agency (NIA), accused the victim of suspected involvement in illegal activities due to the use of a mobile SIM card registered in the victim’s name. The scammer convinced the victim of the alleged illegal activities by engaging in several telephone calls over a period of weeks and eventually prompted the victim to transfer the fixed deposits and transfer the savings to bank accounts for financial verification. The victim became suspicious after the scammer went into hiding and reported the case to the police. Similar cases have been reported in other states. For instance, an elderly woman in Mohali was forced to transfer more than 1.2 crore after the scammer accused her of involvement in terrorist funding and assured her that the amount would be refunded after the completion of the investigation. Another case reported in Bengaluru shows the sophistication of the scam. In this case, the scammer not only conducted video calls with the victim but also sent an individual with the victim’s medication to the victim’s home. The scammer wanted the victim to think that they were being monitored. Eventually, the scammer managed to transfer 50 lakhs. From the cases reported above, it is evident that the cybercriminals are getting more sophisticated in targeting people with more savings. For example, the cases reported above show that the scam targets elderly people and retirees who may not be familiar with the modern types of cybercrimes. Although the cases do not involve the hacking of bank accounts, they rely heavily on the banking system for the transaction and laundering of money.

6.3 SBI’s Position in the Indian Financial System

The involvement of SBI customers in fraud cases receives considerable public interest due to the popularity of SBI, one of the major public sector banks in India, playing a dominant role in retail banking, corporate banking, as well as government-related financial transactions. Due to their wide outreach, cyber fraud cases involving SBI accounts gain considerable media attention.

However, it is worth mentioning that in most cases of digital arrest fraud, the bank's system is not technically compromised. Instead, fraudsters trick customers into making legitimate transactions that appear to be normal from a banking point of view. This indicates that in most cases, fraud is related to the behavioural aspect of financial security. However, banks like SBI are likely to suffer reputational risks in such cases. Customers tend to associate their loss of funds with a bank regardless of whether it is related to the banking system or not.

6.4 Impact on Investor Sentiment and SBI's Stock Price

Cyber fraud cases involving major banks can also impact the market sentiment. Though the financial impact of such a case on a particular bank might be low, there can be a general perception of rising cyber risks, which might impact the long-term operational risks associated with financial institutions. During a recent phase of volatility in the financial markets, SBI shares fell by 5.6 per cent, which resulted in a decline in the valuation of the bank to below 10 lakh crore, as the market capitalisation fell by more than 62,000 crore. Though this fall in SBI shares might not have been due to cybercrime alone, it can be a result of rising concerns regarding financial system risks.

6.5 Wider Implications for the Banking Sector

The digital arrest scam also points out several structural issues faced by the banking sector in the context of the emergence of digital finance. First, the proliferation of digital financial services have resulted in the creation of several avenues for fraud. The emergence of mobile banking services and the development of instant transfer services have resulted in the creation of a financial system where transactions are possible in a matter of seconds. Second, the structure of cyber fraud has also become more structured. For instance, the investigations carried out by Indian law and order agencies have shown that several such scams are conducted by well-knit networks of people who use the services of call centres and fake identity documents. In several cases, the proceeds of such fraud are withdrawn through dozens of bank accounts located across several states.

6.6 Institutional Responses and Preventive Measures

It is observed that banks and financial institutions are taking a few steps to reduce the risks involved with cyber fraud. For example, SBI is conducting customer awareness campaigns about digital arrest scams and other forms of cyber fraud. On one occasion, bank employees prevented a huge loss for a customer by raising suspicions about unusual withdrawals and warning the customer about cyber fraud. Apart from individual bank responses, the Indian government also established the Cyber Fraud Mitigation Centre under the Ministry of Home Affairs. This centre is responsible for responding to cyber fraud by taking into account the responses of banks, telecom operators, and law enforce-

ment agencies. This centre is also working towards increasing the speed of responding to cyber fraud by freezing fraudulent transactions.

From the policy perspective, the solution for cyber fraud involves the application of technology and behavioural solutions. Banks are increasingly adopting artificial intelligence-based solutions for the detection of cyber fraud. Nevertheless, as the arrest scams are based more on social engineering than the actual hacking of the system, the solution may not lie with the application of technology alone. Education of the customer is an important aspect of the solution for cyber fraud. Public awareness programs that help people understand the common practices of fraudsters may help reduce the effectiveness of the arrest scam.

6.7 Human Consequences of Financial Cyber Crime

While financial cybercrimes are often analysed in terms of their financial impact, it is also important to understand that there is a human factor involved in such cybercrimes. Some of the human victims of cyber fraud include elderly people who spend their savings due to high levels of psychological pressure. In several cases, victims have also complained of emotional upsets, embarrassment, and low confidence in internet banking. From a broader societal point of view, such cybercrimes can also affect public trust in financial institutions as well as internet banking in general. Trust is a critical factor underlying financial systems, and once it is breached, it requires a considerable amount of time to rebuild it.

6.8 The Road Ahead

The rise of digital arrest scams represents a major challenge to the banking system of India. Despite the fact that such fraud does not involve a direct breach of banking systems, it represents an exploitation of the interplay between digital technology, human psychology, and financial systems. Incidents involving customers of large banking institutions, such as State Bank of India (SBI), serve to illustrate the overall impact of cybercrime in a more digitized financial system. The overall impact of such fraud is not limited to those who fall victim to such cybercrime. Media reporting, investor psychology, and overall concerns regarding cybersecurity can serve to impact financial markets, as well as fluctuations in the overall valuations of banking institutions. As has been seen through fluctuations in SBI's share value during times of high financial sensitivity, cybersecurity has become a factor in overall financial analysis.

For policymakers and financial institutions, therefore, the task ahead is to devise a comprehensive strategy that incorporates technological security measures, regulatory control, and public education. Improving inter-institutional coordination between banks, communication service providers, and law enforcement agencies will be instrumental in dismantling the infrastructure that supports cyber fraud schemes. Ultimately, the digital

arrest scam serves to reinforce the notion that financial technology development must be matched by equally impressive strides in cybersecurity and consumer protection. With financial systems increasingly moving into the digital age, maintaining public trust will require not just technological ingenuity but also institutional capabilities to provide protection from cybercrime in its various forms.

7. CONCLUSION

Cyber fraud has emerged as one of the most concerning issues in the contemporary financial environment. With rising dependence of the global economy on technology, financial transactions are no longer conducted through conventional physical means but rather through online platforms, mobile banking and electronic money transfer services. On the one hand, incorporating technology has heightened the efficiency, ease of access, and financial inclusion for several stakeholders, whereas on the other hand, it has also increased the global financial system's vulnerability to cybercriminals. In this regard, cyber fraud has become more complex, extensive, and sophisticated, impacting a wide range of stakeholders, from ordinary citizens to financial institutions, organisations, and even countries around the world. Cyber fraud can be addressed through multiple perspectives that incorporate technology, regulations, institutions, and awareness.

The digital transformation of the banking sector, the growing e-commerce platforms, and FinTech have completely changed the face of the financial sector. The innovation in the banking sector gives access to seamless services to all its stakeholders. However, this ease of access has also opened the door for cybercriminals to exploit system vulnerabilities through phishing, identity theft, malware, social engineering, account takeover, and payment fraud. Cyber fraud is no longer a sporadic event; it has become sophisticated, global crime rings that leverages advanced technology. With the rise in global connectivity, the threat of cyber fraud is also increasing, and thus fraud detection and prevention tools have become a high significance.

Detection mechanisms are essential in ensuring that the effects of cyber fraud are reduced. Contemporary fraud detection technology is increasingly dependent on data driven technologies such as artificial intelligence, machine learning, behavioral analytics and the big data analytics. These technologies ease the detection of fraud in real time and to identify the anomalies in the transactions. Advanced fraud detection technology can monitor user behavior, analysing transaction history, and alerting user to potential threats before they result in financial losses. Automated monitoring systems also enable banks to respond to threats more effectively.

However, the banking sector also engages in active adoption of prevention mechanisms along with the detection measures. Prevention measures are designed to lower the chances of fraud occurrences by enhancing the security and assuring its implementation with various levels of authentication. Banking sector is shifting to higher security measures

like biometric authentication, multi-factor authentication, encryption and higher secured channels of online transactions. Customer awareness campaigns also play a vital role in preventing cyber frauds. The cybercriminals utilise the gullibility of the customers to engineer tactics to commit these crimes. Regulatory bodies and banking sector in general engage also in improving the user awareness about the security measures of online transactions. These initiatives also play a significant role in curtailing cybercrimes.

Digital transformation has greatly improved the detection and prevention of cyber fraud. Technological advancements have allowed financial institutions to develop strong cybersecurity systems and enhance their capability to observe and respond to fraudulent activities. Cloud computing, artificial intelligence, blockchain technology, and analytics are some of the most effective technologies that can be leveraged to improve fraud management systems. For instance, AI-based systems can learn from past fraud data and improve their predictive models with time. Blockchain technology also improves the transparency and immutability of financial transactions, making it less vulnerable to fraudulent activities.

Another critical advantage that banking sector draws from digital transformation is the ability to employ integrated systems for security. As financial services extend to mobile applications, internet banking, digital wallets and other platforms, banks now implement an integrated system for cybersecurity, which enables them to track all transactions across all platforms at once. Another significant advantage is that digital transformation enables banks to partner with FinTech companies, cybersecurity companies, and regulatory bodies to develop and implement new solutions to detect, combat and prevent cyber frauds. Worldwide the role of cybersecurity in financial systems is gradually being recognised by the government and the regulatory bodies. International cooperation and regulation are essential to combat cyber frauds, as cybercriminals often operate across borders. Bodies such as the financial regulatory agencies and international cybersecurity associations promote cooperation and collective action against cyber threats. Most countries have adopted stringent data protection regulations and mechanisms and cybersecurity requirements to make banking sector more resilient against cyber threats. However, the dynamic nature of the cyber threats requires constant upgrades and continued improvements to mitigate the emerging challenges.

In India, the development of digital financial services has led to a major shift in the banking and payment mechanisms. The government's initiatives to promote digital payments, financial inclusion, and digital identity solutions have increased the pace of adoption of the e-payment platforms. With the increasing penetration of the mobile banking, real-time payment systems, and digital wallets, the span of individuals accessing the financial services through these mechanisms has increased by manifold. This development and growth have increased the financial services sector and the accessibility among the various stakeholders but also brought with it heightened vulnerabilities.

The banks have developed sophisticated monitoring systems, improved authentication processes and upgraded transaction security procedures to safeguard their customers. Regulatory bodies regularly inform the banking sector of the effective cybersecurity practices, help perform risk assessments, and establish well-developed frameworks for incident reporting. Moreover, the government along with the regulatory bodies engage in increasing the awareness on online safety and fraud prevention methods and launch initiatives at a national level. The Indian financial system has adopted numerous proactive measures combined with the help of the regulatory body to ensure detection and prevention of cyber frauds. Despite these efforts, the number of cybercrimes has increased post the pandemic period. Cybercriminals continue to evolve and adopt new tactics based on the changing trends in customers and their evolving lifestyles. The changes in the financial industry and the proactiveness to shift to the online platforms of banking services has opened a new window of opportunities for cybercrimes. In addition to these, the developing countries face additional challenges, including the lack of expertise, infrastructure, and digital literacy among the population. The prevention of cybercrimes lies in the ability of the banking sector and the regulatory bodies to develop adaptive strategies and for other stakeholders in being conscious while adopting the recent technologies.

REFERENCES

1. Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, 27 (3), 945–958.
2. Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of xidian university*, 14 (7), 1523–1536.
3. Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behavior in e-banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 7 (1), 70–78.
4. Anderson, R., Barton, C., Boehme, R., Clayton, R., Van Eeten, M. J. & Levi, M., Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer.
5. Arcuri, M. C., Brogi, M. & Gandolfi, G., et al. (2017). How does cybercrime affect firms? the effect of information security breaches on stock returns. In *Itasec* (pp. 175–193). Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure no solution. In *Combating cybercrime and cyberterrorism: Challenges, trends and priorities* (pp. 135–155). Springer.
6. Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12 (6), 1333.
7. Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Varstvoslovje: Journal of Criminal Justice & Security*, 16 (2).
8. Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. *International Review of Economics & Finance*, 99, 104053.
9. Chhabra Roy, N., & Prabhakaran, S. (2025). Cyber fraud (cf) in banking: a dual-layer, blockchain-enabled approach for prevention and managerial response. *Managerial Finance*, 51 (5), 765–796.

10. Cobos, E. V., Cakir, S., Straub, S., Qiang, C., & Torgusson, C. (2024). A review of the economic costs of cyber incidents. *World Bank, Washington, DC, USA, Rep*, 193919.
11. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, 44, 100977.
12. Kannan, S., & Somasundaram, K. (2017). Autoregressive-based outlier algorithm to detect money laundering activities. *Journal of Money Laundering Control*, 20 (2), 190–202.
13. Karagozoglu, A. K. (2021). Novel risks: A research and policy overview. *Journal of Portfolio Management*, 47 (9), 11–34.
14. Kwilinski, A., Lyulyov, O., & Pimonenko, T. (2023). Unlocking sustainable value through digital transformation: An examination of ESG performance. *Information*, 14 (8), 444.
15. Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage.
16. Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *Journal of economic literature*, 52 (1), 5–44.
17. Ma, K.W.F., & McKinnon, T. (2022). Covid-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, 29 (2), 433–446.
18. Naidoo, R. (2020). A multi-level influence model of covid-19 themed cybercrime. *European Journal of Information Systems*, 29 (3), 306–321.
19. Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters? *International Journal of Financial Engineering*, 8 (02), 2150019.
20. Njeru, P., & Gaitho, V. (2019). Investigating extent to which cybercrime influences performance of commercial banks in Kenya. *International Journal of Economics, Commerce and Management*, 7 (8), 489–514.
21. Prashanth, B., Kumar, M., Hoque, A., Al Muraqab, N., Moonesar, I. A., Braendle, U. C., & Rao, A. (2026). Prediction of bank transaction fraud using tabnet—an adaptive deep learning architecture. *International Review of Economics & Finance*, 104916.
22. Riek, M., & Bo`hme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4 (1), ty004.
23. Singh, K. N., & Misra, G. (2023). Victimisation of investors from fraudulent investment schemes and their protection through financial education. *Journal of Financial Crime*, 30 (5), 1305–1322.
24. Stango, V., & Zinman, J. (2009). Exponential growth bias and household finance. *The Journal of Finance*, 64 (6), 2807–2849.
25. Stella, G. P., Filotto, U., & Cervellati, E. M. (2021). Financial literacy in Italy: empirical evidence and theoretical proposals. *Sumy: Virtus Interpress*. doi: <https://doi.org/10.22495/flietp>.
26. Walter, I. (2013). The value of reputational capital and risk in banking and finance. *International Journal of Banking, Accounting and Finance*, 5 (1-2), 205–219.
27. Walter, I. (2016). Reputational risks and large international banks. *Financial Markets and Portfolio Management*, 30 (1), 1–17.
28. Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse1. *MIS quarterly*, 37 (1), 1–20.
29. Xu, J. (2024). Ai in esg for financial institutions: An industrial survey. *arXiv preprint arXiv:2403.05541*.