Graphic Era Hill University
DEHRADUN CAMPUS

ISSN: 3049-4311 (Online)

GEHU LAW REVIEW

A Journal of Contemporary Legal Research

Volume & Issue:
Volume [I], Issue [I]

Publication Period:
June 2025

Institutional Affiliation:
School of Law, GEHU Dehradun, Uttarakhand, India

LIST OF JOURNAL ARTICLES

E-Banking Frauds: A Comparative Analysis of Legal Frameworks in India and the USA

Ms. Nidhi Gupta
Ph.D. Scholar
Uttaranchal University
Dehradun

Abstract

A sound and effective banking system is the foundation of any economy, without which it cannot exist. For this, banks play a remarkable role as the main participant, allowing individuals as well as businesses to manage and have access to their finances. The modern banking industry provides ample facilities and opportunities to their customers that have changed the financial landscape as compared to the traditional rule-based banking. Though the digitalization of the entire banking system has undoubtedly revolutionized the financial sector, offering a lot of convenience and accessibility to a number of banking services in just one click, it has also introduced significant vulnerabilities that are exploited by the cybercriminals leading to an increase in the number of e-banking frauds. The quality of e-banking services offered by banks gives a lot of satisfaction to its customer base, but it has also received due attention because of the advent of new challenges posed by the fraudulent behavior of the cybercriminals. That's why it becomes crucial for the evolvement of such a robust and effective mechanism to overcome such activities. The paper delves into the insight of e-banking frauds, reports of government highlighting the increase of such frauds in India and the USA. The purpose of this paper is threefold: firstly, to give an overview of the types of e-banking frauds prevalent in banking institutions; secondly, to comprehensively analyze the legislative measures adopted in India and USA; and thirdly, to suggest practical recommendations and propose the adoption of technological advancements such as artificial intelligence, machine learning, blockchain technology, etc., for combating e-banking frauds effectively and efficiently.

Keywords: Banking System; E-Banking Frauds; Legislative Measures; Technological Advancements; Artificial Intelligence.

Introduction

A well-functioning banking system is the foundation of a sound economy, as it is significant for the economic growth and progress of the country. Various economic factors have influenced the banking sector and services provided by them to their users, and since the emergence of technology, the banking sector has explored new opportunities and keeps on expanding even beyond national boundaries[15]. This has benefited not only the banks but also the customers. It all started with the introduction of credit/debit cards, concept of the internet and online banking, the Electronic Fund Transfer[16], and Real-Time Gross Settlement (RTGS). But the introduction of information technology in the form of e-banking services and its enabled services has changed the outlook of the banking sector, making it convenient as well as easy for the customers to have access to the banking in just a single click[17]. Despite the growth and expansion, it has to face many complexities evolved out of it that mainly include cyberattacks in the form of credit card fraud, information theft, phishing, spoofing, SIM swap, etc., where cyber fraudsters hold no boundaries and it increases with time.

The first focus of this paper is to highlight the rising sparks of cyber criminality, especially in the banking sector, by taking into consideration various governmental reports published by different agencies and explaining different categories of electronic banking frauds such as identity theft, malware, phishing, spoofing, etc., as they pose a major challenge in the smooth functioning of banking services that affects the reputation of the banks.

The article aims to comprehensively analyze the legislative measures adopted in India and the USA, as in India, the legal framework revolves around the Information Technology Act, 2000, the Indian Penal Code, 1860, and the Payment and Settlements Act, 2007, which governs different categories of electronic banking frauds, whereas the USA employs a robust, sound, and effective legislative approach such as the Electronic Fund Transfer Act, Gramm-Leach-

[15] Shefali Saluja and Arjun J. Nair, "An Analysis on Frauds Affecting the Financial Security of the Indian Banking Sector: A Systematic Literature Review", Ethical Marketing Through Data Governance Standards and Effective Technology 1-18 (IGI Global Publishing, 2024)

[16] Chirag Baheti, "E-Banking Overview of Laws in India and Challenges" SSRN 5 (2023) https://ssrn.com/abstract=4428446 or http://dx.doi.org/10.2139/ssrn.4428446.

[17] Iftikhar Ahmad, Shahid Iqbal, Shahzad Jamil, and Muhammad Kamran, "A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques," 2 Linguistica Antverpiensia 3509-3517 (2021).

Bliley Act, etc. The framework deployed by the United States emphasizes consumer protection, data privacy, and stricter penal provisions holding a benchmark for other countries.

The overall findings of the paper are clubbed together into practical suggestions as to what could be the probable changes that could be made in the existing provisions so as to combat the menace of banking frauds and to make recommendations in the form of the adoption of AI and its aligned technologies, such as machine learning and blockchain technology, that could be adopted with a view to enhancing and safeguarding India's future digital perspectives. All these will contribute a sound as well as a significant contribution for the researchers to look into this concerned area and enhance the quality of further research.

Methodology

The design and execution of this study have been based upon the doctrinal method. A systematic approach has been adopted to collect, analyze, and synthesize the existing literature for this review article. Secondary sources have been collected, which are the main source of information for this study. A comprehensive search was made across different academic publications, reference books, conference papers, and database sources such as Scopus, JSTOR, and Google Scholar. Peer-reviewed journal articles, government reports, and relevant legal texts are searched and it was limited only to two countries, i.e., India and the USA. And in order to enhance the clarity, tables and charts have been used. Conclusions and proposed recommendations are based on the discussions and findings derived from the analysis of the review article, creating a foundation for future researchers willing to work in this field.

Electronic Banking Frauds and Its Types

The evolution of e-banking in this era has suddenly changed the realm of the banking sector and simultaneously increased the number of cyber threats and financial frauds. On a worldwide scale, there has been a critical concern over the susceptibility of financial institutions and their customers when it comes to cyberattacks[18]. Recent trends can be seen in the malware evolution that requires continuous effort to make a sound and effective change in the existing banking

[18] Swati Gupta, "Hacking the System:A Deep Dive into the World of E-Banking Crime" in Gagandeep Kaur, Tanupriya Choudhury, S. Balamuruga, The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0 (2025)

security paradigms that are currently in use. Following are the different categories of e-banking frauds that are prevalent in both countries.

UPI frauds

UPI is a mobile-based digital payment system, developed by the National Payments Corporation of India, which has revolutionized the digital transaction landscape in India, but it has also brought certain challenges in the form of several fraudulent operations[19]. It is clear from the data provided by the NCPI that UPI and banking frauds are the most targeted among all that occurred during the period from January 2020 till June 2023[20].

Debit/ Credit Card Frauds

Innovative technologies and communication methods has resulted in a serious and growing problem, which includes contactless payments via credit or debit cards. Cyber fraudsters are mainly concerned with the use of such sophisticated technology, with the help of which they can conduct illegal transactions[21]. Here, fraudulent transactions are carried out while making online purchases.

Identity Theft

One of the common types of e-banking fraud is identity theft, which is a criminal act where the fraudsters use another person's personal information, though wrongfully obtained and without consent, and it is used for fraudulent purposes[22]. Such incidents are increasing at an alarming rate; therefore, it becomes crucial to protect one's digital identity while minimizing the impact of identity theft.

[19] S. Jagadeesan, K.S. Arjun, G. Dhanika, G. Karthikeyan, K. Deepika, "UPI fraud detection using machine learning," Challenges in Information, Communication and Computing Technology (2024)
[20] "Financial fraud top cybercrime in India; UPI, e-banking most targeted: Study." Hindustan Times [Internet]. Sep 18, 2023.
[21] Asma Cherif, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, Abdessamad Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review" 35 Journal of King Saud University - Computer and Information Sciences 145–174 (2022).
[22] Emin Huseynov, "Identity theft." Computer and Information Security Handbook: In Elsevier eBooks 993–1006 (2024) https://doi.org/10.1016/b978-0-443-13223-0.00060-6

Phishing

Phishing is basically a social engineering attack executed/delivered electronically. In this, the perpetrator portrays himself as a genuine and legitimate entity via fraudulent emails, text messages, calls, or websites in order to gain sensitive information from the victim.[23] They even infect the device with malware. They impersonate him as someone whom the victim already knows and trick them into answering some confidential banking information. Some of the common phishing attacks involve QR code phishing, smishing, email phishing, vishing, social media phishing, etc.[24]

Skimming

It usually happens in the case of ATMs where a device is attached to the ATM that reads all the acts performed by the user and records the magnetic strip data stored in the ATM card when they are inserted/put into the ATM vending machine. These devices are difficult to detect because they are designed to blend with the ATMs design, where it becomes invisible for the user to detect it[25].

Fund Transfer Scams

It includes the cases where the fraudsters make fraudulent fund transfers by using real bank data and customer information, and then they execute their plan while funds are being transferred[26]. It occurs whenever a criminal commits an act by which he seizes accounts and transfer funds from an individual's online bank account[27].

[23] Mohsin Kamal, Jahangir Chauhan, Md. Qaiser Alam, Md. Rahber Alam, "Anatomy of Financial Misconduct: A Critical Insight into Key Banking Frauds in India." SSRN Electronic Journal (2025) https://doi.org/10.2139/ssrn.5149325
[24] N.V. Keerthana, P. Suresh, et.al., "Critical Strategies for phishing defense and digital asset Protection." Critical Phishing Defense Strategies and Digital Asset Protection In IGI Global eBooks 221–244 (2025). https://doi.org/10.4018/979-8-3693-8784-9.ch011
[25] Gautham Manoharan Sujatha, Fayaz Ahmed Rahman, et.al., (2025). "ATM skimming device detection using IOT." AIP Conference Proceedings: 3175, 030001 (2025) https://doi.org/10.1063/5.0254592
[26] Henderson, I. (2003). "Electronic funds transfer fraud." 12 Computer Fraud & Security (2003) 6–9. https://doi.org/10.1016/s1361-3723(03)00006-x
[27] Paolo Vanini, Sebastiano Rossi, et al., "Online payment fraud: from anomaly detection to risk management." 9 Financial Innovation, 66 (2023). https://doi.org/10.1186/s40854-023-00470-w

Rising Sparks of E-Banking Frauds in India and USA

There has been a tremendous increase in productivity as well as a competitive advantage because of the improvements made in the digital technologies that have also replaced the physical form of money, i.e. cash, with digital transactions in both countries. Mobile payment transactions are carried out with mobile phones, allowing users to carry out their banking operations such as deposit, withdraw, transfer, and send money from one account to another[28]. All this is made possible by the advancement of technology and interconnected systems, which are so intermingled that it creates opportunities for the cybercriminals to make use of the vulnerabilities prevalent in the system[29].

According to a report 'Cyber Fraud and Digital Harassment[30]', statistical data on categories of fraud for cybercrimes is published by the National Record Crimes Bureau, where it is clearly shown that there has been a surge in the number of cases registered for online banking frauds or scams as compared to other related frauds as shown in Fig.1:

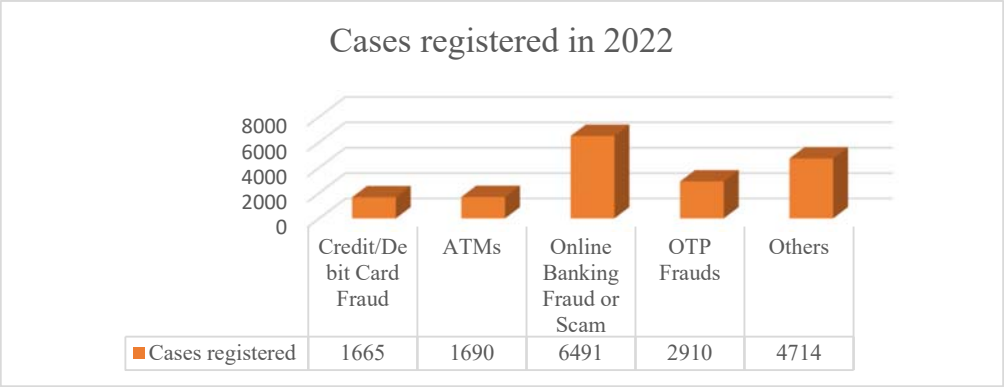

Figure 1. Total Number of E-Banking Fraud Cases Registered in India

While USA is experiencing a sudden growth in the percentage of financial cybercrimes, especially credit card frauds, which is the most frequently reported financial cybercrime, as per

[28] Petr Hajek, Mohammad Zoynul Abedin, et.al. "Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework." 25 Information System Frontiers 1985–2003 (2023). https://doi.org/10.1007/s10796-022-10346-6

[29] Mohammed Afzal, Mohd. Shamim Ansari, et al., "Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach." 29 Journal of Financial Services Marketing 1503–1523 (2024). https://doi.org/10.1057/s41264-024-00279-3

[30] Ministry of Home Affairs, Government of India "Cyber fraud and digital harassment" [Internet]. Press Information Bureau https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186

the reports published in 2023[31], data breaches, account hacking, online banking scam and phishing attacks remained a persistent threat, as portrayed in Fig. 2, that are committed with the sole objective of having unauthorized access to users' accounts and gaining undue advantage by adopting such fraudulent practices.

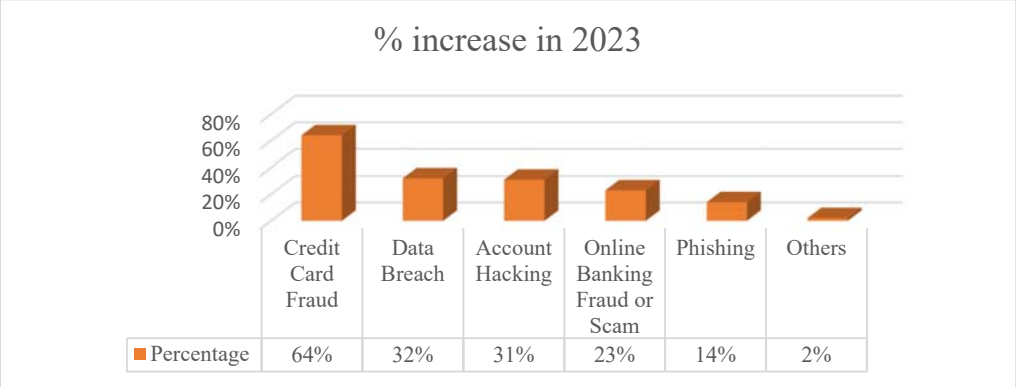

Figure 2. Percentage increase in the E-Banking Frauds in USA

USA's law enforcement agency, the FBI (Federal Bureau of Investigation), part of US Department of Justice, is the nodal agency responsible for handling the investigation of crimes and protecting the country from threats. The agency has evolved a direct way for the public in the form of IC3, i.e., Internet Crime Complaint Centre, to report cybercrimes. IC3 prepares and submits its annual report, where it highlights the number of complaints registered and the amount of loss in those complaints (Figs. 3, 4)[32]. The number of complaints regarding phishing/spoofing is approximately 3 lacs which is increasingly high as compared to other types, and the total amount of losses is comparatively high in comparison to credit card and check frauds, despite the fact that the number of complaints of credit card/check frauds is very low. While the number of complaints regarding SIM swap is at the lowest level, in case of complaint losses, malware attacks hold the least position.

[31] Statista. "U.S. most common financial cybercrime or fraud victims 2023." [Internet]. *Cyber Crime and Security* (2024). https://www.statista.com/statistics/1460422/financial-cybercrime-common-fraud-us/

[32] FBI "Internet Crime Report, 2023" *Internet Crime Complaint Centre* (2023) https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

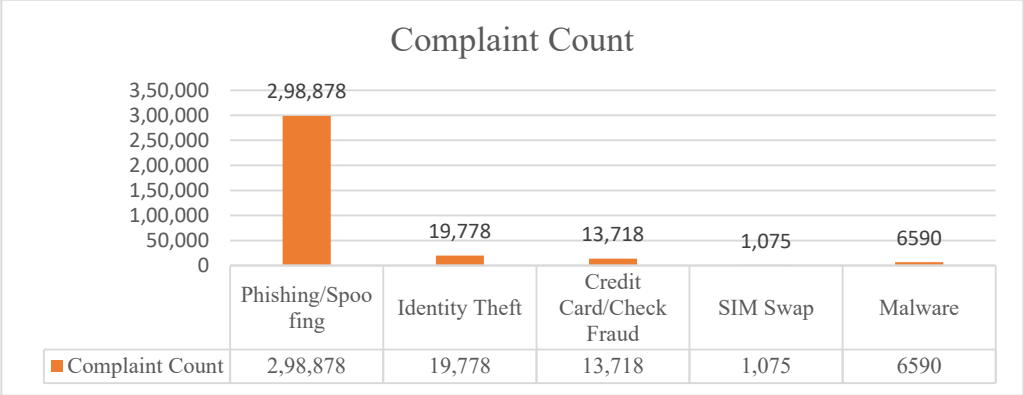

Figure 3. Complaint Counts for different types of e-banking frauds in 2023

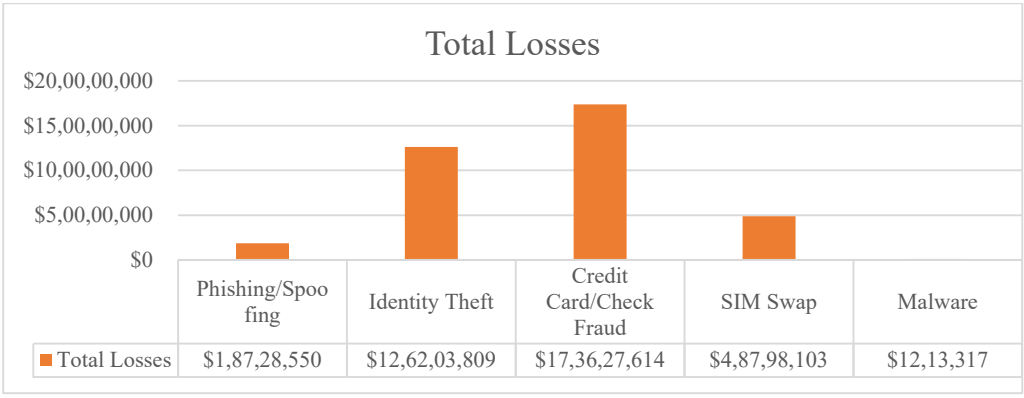

Figure 4. Complaint Losses for different types of e-banking frauds in 2023

The Reserve Bank of India has released a report that states that the number of bank frauds has increased in the last two years, with 29,493 cases registered in FY 2023-2024, and the total amount of money involved in these frauds has declined in FY 2023-24 as compared to FY 2022-2023. Combined data of private sector and public sector banks has been mentioned below (Fig. 5).

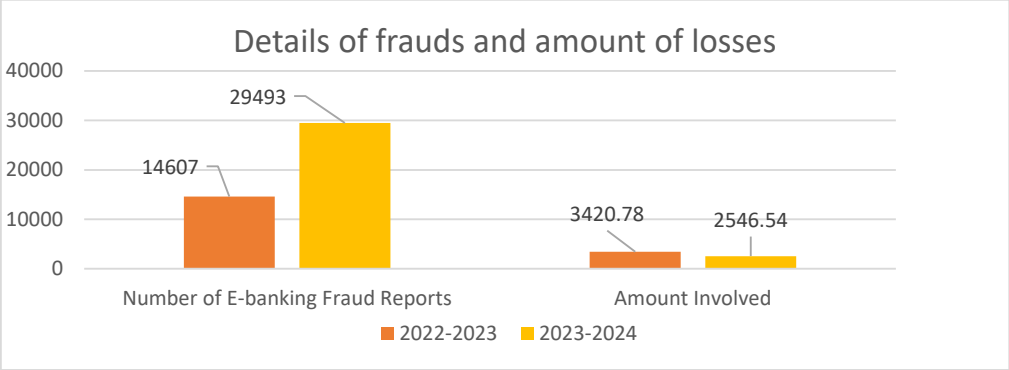

Figure 5: Data of Private Sector and Public Sector Banks combined together

E-Banking Fraud: Legislative Measures Adopted in India and USA

INDIA

Indian Penal Code, 1860 (Act 45 of 1860)

Though the IPC does not specifically deal with the electronic banking frauds, but there are certain offenses which can fall under this category of crimes, such as:

- Section 378 &379- It includes theft related to mobile phones, data as well as hardware/software of the computer systems. It also provides for the legal framework to prosecute all those who are engaged in the commission of cyber theft activities.
- Section 383 &384- Deals with extortion, where a person extorts valuable security or property by putting the person into fear of injury.
- Section 403-406- These sections provide for dishonest misappropriation of property, which includes criminal misappropriation and criminal breach of trust
- Section 463 & 464(c)- Forgery, not only covers false document but also deals with the false electronic records and affixing electronic signature on any electronic record. Offences like spoofing and online forgery are covered under this section. It is punishable with fine or imprisonment or both.

- Section 420- Cheating and dishonestly inducing delivery of property. The offence of fraud is inclusive of all those acts of frauds which are concerned with the password theft, bogus websites creation, cyber frauds. Based on the gravity of the act committed, varying imprisonment and fines are imposed on the defaulter.

Information Technology Act, 2000 (Act 21 of 2000)

In India, the Information Technology Act, 2000 deals with different categories of cybercrimes such as cyber terrorism, cyberbullying, hacking, defamation, damage to computer resources, etc. Apart from this, it also takes into consideration, though not expressly, provisions relating to internet financial frauds. Section 43 of the Act deals with the infliction of penalties and compensation in case of accessing or securing access without due permission, downloading of or copying of data stored in a computer or computer resource, with the purpose of injecting computer viruses or worms into the system, causing damage to computers, illegal access to another's account, etc.[33]. Here it covers the e-banking frauds such as malware attacks, ransomware, ATM fraud, SIM swap, account takeover, card cloning, card skimming, phishing, etc. Section 66 provides a penalty for any act committed under section 43, and whoever does it dishonestly or fraudulently shall be punished with imprisonment for 3 years or with a fine of Rs 5 lakhs or with both[34].

The Information Technology (Amendment) Act, 2008, has added some other cybercrimes. Whoever dishonestly receives stolen computer resources or communication devices shall be held liable for detention for a period of 3 years or with a fine of Rs 1 lakh or with both[35]. Similarly, section 66 C deals with the punishment for the offense of identity theft, where one who fraudulently uses the electronic signature of another person or another unique identification feature[36]. Section 66 D highlights the penalties for the offense of cheating by misrepresenting themselves so as to have access to a computer device or computer resource[37]

[33] Information Technology Act, 2000 (Act 21 of 2000), s. 43
[34] Information Technology Act, 2000 (Act 21 of 2000), s. 66
[35] Information Technology Act, 2000 (Act 21 of 2000), s. 66B
[36] Information Technology Act, 2000 (Act 21 of 2000), s. 66C
[37] Information Technology Act, 2000 (Act 21 of 2000), s. 66D

Prevention of Money Laundering Act, 2002 (Act 15 of 2003)

In 2002, this Act was passed in India to empower the apex banking institution and other statutory authorities such as RBI, SEBI, and IRDA. They come under the aegis of this Act, and thus all the banks, financial institutions, and insurance companies are covered by it. It makes money laundering a punishable offense where the offender will be held liable for rigorous imprisonment up to three years, which may be extended to seven years, as well as fine.

Internet banking and the Payment and Settlements Act, 2007 (Act 15 of 2007)

The Reserve Bank of India has set up a new mechanism, which is known the Payment and Settlement Act System, 2007 so as to empower the apex banking institution. It deals with the situation where electronic funds transfer gets dishonor for insufficiency, etc., of low funds in the account. The punishment provided for the same is imprisonment for a term up to two years or a fine that may extended to twice the amount of the electronic funds transfer or both.

National Cyber Security Policy, 2013

In 2013, the government of India adopted a new policy named as the National Cyber Security Policy that was enacted with the main objective of a digital landscape where cyberspace is secured in the country so that trust and confidence can be gained in the customers transacting through IT systems and cyber technology. The Indian Cyber Regulatory Framework also adheres to this policy. As to ensure more vigilance and attention concerning the e-banking frauds in the country, this policy was adopted.

The Reserve Bank of India Act, 1934 (Act 2 of 1934)

The whole banking system in India is governed by the RBI Act, which is the nodal legislation obliged with the functioning as the country's central banking institution. This Act also does not specifically deal with cybercrime but it has been amended with time to cover the areas of cybersecurity concerns and technological advancements. A number of guidelines have been laid down by the RBI pertaining to the electronic banking services that are most important to be followed. They are—

- Monitoring of frauds above the value of Rs.1 crore.
- Introduction of a separate department concerned with e-banking fraud transactions.
- Establishment of a fraud review council.
- Maintaining decorum by protecting the valuable data of the customers.
- Know Your Customers norms to be adhered to strictly.
- Creating awareness among customers about the e-banking frauds.
- Educate the customers on how to deal with the e-banking frauds.
- Functioning report has to be submitted by the banks to the Reserve Bank of India.
- Preventive measures to be taken while availing e-banking services.
- Periodical research and development as well as training sessions to be conducted for the employees to make them well equipped with the technology with the changing time.

USA

18 U.S. Code § 1344- Bank Fraud

This legislation has been specifically crafted to deal with the situation of fraudulent activities taking place in banking institutions. Section 1344 is mainly concerned with the banking frauds, online forgery, and laws relating to the punishment and fines. Department of Justice with an object of preventing any scheme that might affect a bank.

It provides that if anyone carries out or attempts to carry out a scheme knowingly:

1. With an intention to defraud a financial institution; or
2. Obtaining of money, funds, credits, assets, securities, or other property or securities owned by or under the control of a financial institution through a process of false or fraudulent pretences, representations, or promises, has to bear up a fine of up to $1,000,000, imprisonment for up to 30 years, or both.

Regulation E (Electronic Fund Transfer) 1978

The Electronic Fund Transfer Act (EFTA), 1978 (15 U.S.C. § 1693) is one of the legislations in USA that is meant to protect and preserve the interests of banking customers while

conducting transactions through internet banking mode. This Act also focuses on the rights, liabilities, interests, and responsibilities of consumers against the acts that are incorrect and illegal in nature. Regulation E specifically applied to frauds related to ATMs, direct deposits, money transfers (whether at the national level or at international level), overdraft banking services, gift vouchers, etc. This legislation provides a mechanism for reporting any kind of errors, unauthorized access, transactions and fraud. The Consumer Financial Protection Bureau (CFPB) has been the nodal agency that has been entrusted with the responsibility of imposing civil liabilities on those institutions that violate Regulation E.

The Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030)

This legislation was enacted in the year 1986 in USA, focusing on the prohibition of unauthorized access to any computer system without getting permission from the authorized user or agent. It not only covers private systems but also government systems and addresses the challenges that are faced pertaining to financial records and government information. The provisions of this Act provide protection from illegal and fraudulent access to the computer systems with malicious intention, but this Act only covers an amount that exceeds $5000 annually.

Bank Secrecy Act, 1970

Significant risks have been posed by money laundering acts to the safety and security of the US financial industry, whereby the criminals tend to use money laundering schemes to hide the source of funds obtained fraudulently. Under these laws, banks must adhere to the guidelines requiring the establishment of effective BSA compliance programs and an efficient suspicious activity monitoring and reporting procedure. For this, BSA E-Filing Systems have been established where financial institutions can submit suspicious activity reports[38].

Gramm Leach Bliley Act, 1999

It is a federal law that has been framed with the object of requiring financial institutions to protect and safeguard the identity, privacy, and security as well as the customer's personal

[38] Bank Secrecy Act, 1970 https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html

financial information. Directions are issued by it to the Federal Deposit Insurance Corporation (FDIC) so as to ensure that financial institutions must frame guidelines, procedures, and policies accordingly and prevent any unauthorized transaction from taking place disclosing financial information of the customers and create a sense of fear among the cyber fraudsters when having fraudulent access to such information[39]. It deals with the safeguarding of customer information. Verification procedures, fraud prevention, and information security, as well as the reporting of suspected identity theft and pretext calling.

Analysis and Discussions

- Figures 1, 2, 3, 4, and 5 clearly show that there has been a surge in the number of e-banking frauds in recent times, resulting in losses of huge sums of money. Not only is a single technique used but different tactics such as spoofing, phishing, identity theft, digital arrest, and social engineering are used by them, making it hard for the concerned law enforcement agencies as well as the government to minimize the risk of e-banking frauds.

- Both countries are facing huge monetary and financial losses as well as affecting the inbuilt trust of customers in online banking systems.

- From the above legal provisions, it can be analyzed that there is no single aggressive legislation in India and USA that can demonstrate a clear recognition of the growing threats posed by e-banking frauds. However, India relies on the existing traditional criminal laws, such as the Indian Penal Code, technology-based statutes such as the Information Technology Act, 2000, along with 2008 amendments. While USA, takes into consideration the targeted legislations such as the Computer Fraud and Abuse Act (CFAA) and Regulation E, directly addressing financial crimes and consumer protection in electronic banking. Guidelines and mechanisms have been specifically laid down under these laws but do not expressly provide for every kind of e-banking fraud.

[39] Federal Deposit Insurance Corporation "FIL-39-2001 Attachment USA", https://www.fdic.gov/news/financial-institution-letters/2001/fil0139a.html

- As far as enforcement of these legislations is concerned, India is concerned mainly with the integration of existing frameworks under acts like the Prevention of Money Laundering Act (PMLA) as well as the guidelines that were issued by the Reserve Bank of India (RBI). However, USA provides for more stringent legislation, such as the Bank Secrecy Act, that provides for a mature enforcement mechanism by which suspicious transactions can be detected and reported.

- Lack of awareness among the customers regarding the probable consequences of e-banking frauds makes them more vulnerable to evolving tactics of cybercriminals.

Recommendations

- While both countries have made significant efforts in addressing these fraud challenges. However, the Indian legislative framework can make efficient and effective changes by adopting certain practices prevalent in USA, such as:

    a. Introduction of a clear reporting and compensation process, similar to that of Regulation E, that can strengthen consumer protection mechanisms.

    b. CBI (Central Bureau of Investigation) and other specialized cybercrime agencies should be established just like USA's FBI (Federal Bureau of Investigation) and must be given jurisdiction-specific authority for proper enforcement mechanisms.

    c. Level of awareness to be enhanced among the customers by increasing financial literacy campaigns about e-banking fraud prevention.

- Both countries should evolve a comprehensive data protection law that can protect the confidential financial data of the customers. USA can dive into and draw inspiration from India's regulatory integration established under the RBI, which establishes accountability and transparency.

- Inclusivity must be the focus so as to bridge the enforcement disparities that might exist in the banking and financial institutions.

- Both countries should allocate their resources in consumer awareness campaigns and programs, and focus should be made on stronger encryption and multifactor authentication.
- Global collaboration and cooperation are required to tackle cross-border frauds, as the main problem lies in the fact that the culprits are not prosecuted because of jurisdictional problems.
- Comprehensive steps such as instituting a robust internal audit and control framework have to be taken to keep an eagle's eye view on the fraudster's next step while committing e-banking frauds.
- Technological advancements such as integrated AI with blockchain technology, machine learning algorithms such as decision-tree, fuzzy-logic can be adopted that helps in reporting real-time e-banking frauds well in advance.

Conclusion

A comparative study with respect to e-banking fraud laws in India and USA reveals that both economies are growing at a very fast pace, similarly looking after the growing threats of cyber fraud. Though both countries face similar types of banking frauds electronically, but substantial difference can be seen in the legal frameworks, enforcement mechanisms, and technological approaches adopted. A well-established legal system and advanced technological fraud detection in USA help them in providing robust protection against e-banking frauds. While in India, significant progress can be seen from the fact that there has been rapid evolvement of legal frameworks and regulatory policies in this domain. But lack of sincere efforts on the part of the judiciary as well as limited public awareness creates obstacles in the achievement of the sustainable digital ecosystem. Not only India and USA but also collaborative participation, exchange of best practices, and adoption of technological innovation are the need of the hour that would ensure securing a robust e-banking system in this increasingly interconnected financial world. As digital transactions are growing exponentially, it becomes crucial to prioritize cybersecurity so that trust and confidence of people in the e-banking systems is maintained worldwide.