THE ROLE OF LAW AND TECHNOLOGY IN COMBATING DIGITAL BANKING FRAUDS IN INDIA

Prof. (Dr.) Seema Surendran, Professor, CMR University, School of Legal Studies, Bangalore, Karnataka

Niriksha Y M, LL.M. (Commercial Law), CMR University School of Legal Studies, Bangalore, Karnataka

ABSTRACT

Digital banking has transmuted India's financial landscape, providing ease and accessibility like never before. However, this drastic change has also led to a surge in fraudulent activities, exploiting vulnerabilities in digital transactions. Cybercriminals employ various deceptive techniques, including phishing, vishing, spear phishing, skimming, SIM swaps, and malware attacks, to manipulate unsuspecting individuals and financial institutions. The Reserve Bank of India reported a nearly 300% increase in bank fraud cases during the financial year 2023-24, emphasizing the growing threat posed by digital payment frauds. This alarming rise calls for comprehensive legal and technological safeguards to protect consumers and financial institutions alike. Strengthening cybersecurity frameworks, enhancing fraud detection mechanisms, and promoting digital literateness among users are crucial steps in mitigating these risks. This paper explores the legal framework established to combat digital banking frauds and examines the part of technology in addressing these challenges. The study explores into the legal and regulatory division surrounding digital banking frauds in India, examining key legislation, judicial precedents, and enforcement mechanisms. It also explores technological developments such as artificial intelligence, blockchain, and biometric authentication, assessing their role in enhancing security and fraud prevention.

Keywords: Digital Banking frauds, Reserve Bank of India, financial sector, technology, regulatory framework, challenges.

1. Introduction

The Indian banking area aids as a cornerstone of the country's economic development, facilitating industrial growth, employment generation, and financial inclusion. Over the years, various reforms have strengthened the efficiency and stability of banking institutions, ensuring a stronger financial system. The sector plays a fundamental role in channelling monetary resources to businesses and individuals, thereby fostering economic progress. In spite of these advancements, the banking industry faces persistent challenges. The rise in non-performing assets (NPAs), the growing pervasiveness of digital frauds, and the limited convenience of banking services in rural areas remain demanding concerns. Addressing these issues requires a multi-faceted approach, including stringent regulatory oversight, enhanced fraud detection mechanisms, and expanded financial outreach programs. India's banking landscape is diverse, comprising public-sector banks, private-sector banks, foreign banks, regional rural banks, and cooperative banks, all regulated by the RBI. The dawn of globalization and digitalization has revolutionized banking operations, making financial services more reachable and efficient. E-banking, which encompasses online transactions, mobile banking, ATMs, and electronic data exchange, has significantly improved customer convenience[1]. By leveraging secure digital platforms, banks can offer seamless financial services, ensuring accessibility anytime and anywhere. The objectives and purpose of this study is mainly to look into to analyse the efficiency of existing legal and regulatory measures in combating Digital Banking Frauds in India, to understand the extent and the impact of Digital Banking Frauds on consumers as well as financial institutions in India and to analyse the use of technology in detecting and preventing Digital Banking Fraud.

2. History And Development Of E-Banking in India

The evolution of e-banking in India has been a transformative journey, reshaping the financial sector and enhancing accessibility for millions. The initial adoption of electronic banking in the **20th century** focused on basic services such as bill payments, account inquiries, and fund transfers. However, the late **1990s and early 2000s** marked the emergence of digital banking, introducing online functionalities like balance checks and cash transfers[2]. The **2010s** witnessed a momentous shift with the widespread use of smartphones and net connectivity, leading to the

[1] Dinesh Dayma, Cyber Frauds: A Growing Threat to Indian Banking Sector & Preventive Strategies, 6 INT'l J.L. MGMT. & HUMAN. 794 (2023).
[2] Chandrawati Nirala, Dr, BB. Pandey, 'Evolution of e-banking in India- An Empirical Study

rise of mobile banking applications. A major milestone came in **2016** with the launch of the **Unified Payments Interface (UPI),** which revolutionized digital transactions by enabling unified fund transfers between bank accounts. During the mid-2010s, fintech startups played a vital role in expanding financial inclusion, offering innovative solutions in payments, lending, and wealth management. These startups focused on connecting the gap between traditional banking services and underserved communities, making financial services more accessible. The **COVID-19 pandemic in 2020** further accelerated the shift toward digital banking, as lockdowns and safety concerns drove a surge in online transactions. Banks responded by upgrading their digital platforms to meet the growing demand for contactless financial services.[3] Government initiatives such as **Jan Dhan Yojana** supported this digital transformation, aiming to create a more inclusive financial ecosystem. The **RBI** played a crucial role in shaping the regulatory framework, introducing guidelines to enhance transaction security and protect customer data. Additionally, the RBI modernized it's **Know Your Customer (KYC)** processes, enabling remote verification through Aadhaar and other digital methods.[4]

India's financial growth in the early 2000s created a demand for more accessible and convenient banking services. The speedy advancement of technology and the widespread availability of the internet have significantly influenced the banking sector in India. Financial institutions have embraced digital banking solutions, making transactions more accessible and efficient for individuals and businesses and its privileges can be measured in terms of improved processing rapidity, communication rates and access time[5]. This shift has transformed the way people manage their finances, integrating digital banking as a fundamental component of the financial ecosystem. While digital banking has introduced convenience, it has also led to an increase in fraudulent activities, posing serious security challenges. Cybercriminals employ various tactics such as phishing, malware attacks, identity theft, and social engineering to exploit vulnerabilities in online banking systems. Understanding the connection between technological advancements and banking frauds is crucial in developing effective mitigation strategies.

[3] Prashant Singh Rajput, Evolution of Banking System in India, 4 J. Contemp. Issues L. 49 (2018).
[4] Ibid
[5] Monica N. Agu, Challenges of Using Information Technology to Combat Economic Crime, 6 AFR. J. COMP ICTs 31, 31-35 (2013).

To combat these threats, financial institutions and regulatory bodies must implement robust security measures. Strengthening regulatory frameworks, adopting advanced authentication mechanisms, investing in fraud detection systems, and promoting cybersecurity awareness are essential steps in safeguarding digital transactions. Despite the progress in digital banking, cybersecurity and data protection remain significant concerns. Existing laws and regulations have gaps that need to be addressed to effectively combat digital banking frauds. Strengthening legal provisions and enhancing enforcement mechanisms will be key in ensuring a secure banking environment.

However, this transformation also brings challenges, as cyber threats continue to rise. The growing prevalence of digital banking frauds highlights the need for strong legal frameworks to protect consumers and maintain the integrity of the financial system. Fraudsters exploit weaknesses in digital platforms through various unlawful activities, including phishing, identity theft, hacking, malware attacks, and social engineering scams[6]. By leveraging sophisticated techniques, they gain unauthorized access to sensitive financial information, making fraud prevention a top priority for financial institutions.

3. Types of Digital Banking Frauds

Online Banking Frauds encompass various tactics used by criminals to lure money or sensitive information which includes various types such as:

a.) PHISHING: Phishing is a type of cyberattack also called as Carding and Spoofing in which scammers send emails through phone in the name of a reputable financial institution/bank[7]. Frequently, these emails include links to websites that mimic legitimate financial gateways. Customers' login credentials are stolen by the attackers, who then have unauthorised access to their accounts. For example, A consumer gets an email pretending to be from their bank warning them that if they do not update their information, their account would be blocked. Clicking on the link redirects them to a

[6] https://www.stthomas.edu/publicsafety/prevention/fraudidtheft/Phishingpharmingvishingsmishing /

[7] In one such instance in August 2003 a bulk e-mail was received by customers of Citibank asking them to visit its official website and agree to change policies. The URL link www.citibank.com took place the recipient not to the Citibank site but to some other site where the user was asked to certain personal details. The UK strengthened its legal arsenal against phishing with the Fraud Act, 2006, which introduces a general of fraud that can carry up to three-year prison sentence and prohibits the development or possession of phishing kits with intent to commit fraud.

fake banking page where they unknowingly enter their username, password, and OTP, allowing fraudsters to access their bank account.

b.) SIM SWAP FRAUD: In SIM Swap Fraud, thieves obtain a fake SIM card from the telecom operator to take control of a victim's mobile number. After obtaining the SIM, they can reset passwords and gain access to the victim's bank accounts. For Example, using fictitious identification, a scammer contacts the cell service provider pretending to be the victim and asks for a replacement SIM card. Once engaged, all bank notifications and OTPs are sent to the fraudster, who uses them to carry out fraudulent activities without the victim's knowledge.

c.) UPI FRAUDS & QR CODE SCAMS: Scammers use fictitious payment requests or QR codes to fool victims into authorising fraudulent transactions over the Unified Payments Interface (UPI). In online marketplaces, scammers frequently pretend to be purchasers and send QR codes, claiming they need them to "receive" money. However, scanning the code takes money out of the victim's account. Example: A scammer impersonating a buyer sends a QR code after a seller offers an item on OLX, stating it is for payment receipt. By scanning it, the vendor unintentionally approves a debit transaction rather than a credit one, resulting in the loss of money.

d.) REMOTE ACCESS SCAMS: Fraudsters utilise remote access programs like AnyDesk, TeamViewer, or QuickSupport to trick victims into installing them which may remotely control their equipment. Once installed, scammers can access financial apps, steal login information, and carry out illegal activities. For instance, a victim receives a call from a person posing as a customer service representative from a bank. In order to resolve a "security issue" with the bank app, they request the user to install AnyDesk. After installation, the fraudster gains control of the device and withdraws funds from the victim's bank account.

e.) BANKING MALWARE & TROJANS: To obtain sensitive financial information, fraudsters use trojans and malicious software (malware) to infiltrate a user's computer, smartphone, or banking app. [8]These malicious apps have the ability to override two-factor authentication, login credentials, and record keystrokes and this is nothing but

[8] P. TAYLOR, Hacktivism: In Search of Lost Ethics, J. HUM. TTS PRAC., Nov. 2015, at 625-646

hacking and computer manipulations. For instance, a user installs a fraudulent app from an unreliable source, believing it to be a legitimate banking app. After installation, the malware records the user's OTPs and login information, enabling hackers to access the account and drain it.

f.) VISHING: Here, scammers pose as bankers, business executives, insurance agents, government representatives, and others in order to contact or approach clients via social media or phone calls. Imposters divulge a few customer details, including the customer's name or birthdate, to bolster their confidence. By claiming an urgency or emergency, such as the necessity to stop the illegal transaction, the requirement to pay to avoid penalties, or an alluring discount, imposters may coerce or deceive victims into divulging private information like passwords, OTPs, PINs, and Card Verification Values (CVVs). Customers are then conned using these credentials.

g.) DENIAL OF SERVICE ATTACK (DoS): A DoS attack involves an attacker deliberately overwhelming a network or server with an excessive number of requests, with the intent to disrupt its operations and cause harm. This results in the targeted online services becoming inaccessible, altering the state of the digital property and reducing its value or functionality. For instance, a website going offline can lead to financial losses, damage to reputation, and interruptions in operations for the affected organization. The network, server, or online service targeted in the attack is treated as property, and the assault compromises its utility and effectiveness.

CREDIT/DEBIT CARDS	**ATM's**	**ONLINE BANKING FRAUDS**	**OTP FRAUDS**	**OTHERS**	**TOTAL**
1665	1690	6491	2910	4714	17,470

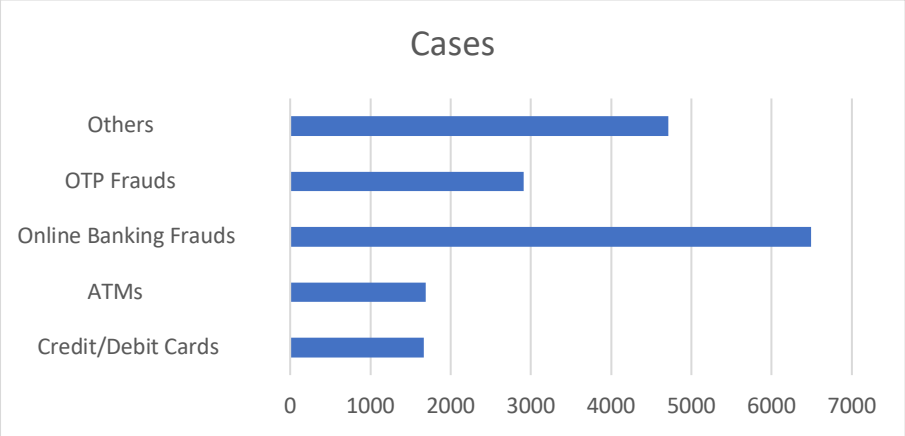

FIGURE 1: Report from The National Crime Records Bureau (NCRB) for the period 2022

In the above-mentioned statistical data by The National Crime Records Bureau (NCRB) for the year 2022 published in the "Crime in India" publication clearly states about the cases recorded under Fraud for Cybercrimes it is observed that about 6,491 cases have been registered for Online Banking Frauds 2,910 cases regarding OTP frauds 1,690 cases ATM frauds and 1,665 Credit /Debit card cases that have been brought before the NCRB.[9]

4. Legal Framework Governing Digital Banking Frauds in India

In India, the swift adoption of digital banking services has increased the urgency for effective measures to prevent and address digital banking frauds. The country's legal framework is crucial in tackling these issues, offering the necessary legal foundation for regulating electronic transactions, ensuring data protection, and bolstering cybersecurity. This framework includes a mix of legislative measures, regulatory guidelines, and oversight by specialized authorities.

4.1 Information Technology Act, 2000

This act administers different parts of electronic trade and cybercrimes in India. It incorporates arrangements connected to hacking, information burglary, and online fraud. The Information Technology Act, 2000 (IT Act) fills in as the essential regulation administering different parts of electronic trade, network safety, and cybercrimes, including online banking frauds. Sanctioned to work with online businesses, directly advanced marks, and give legitimate acknowledgment to electronic exchanges, the IT Act contains provisions like section 46,

[9] Press Information Bureau, Government of India, "Press Release," January 31, 2025, https://pib.gov.in/PressReleasePage.aspx?PRID=2080186.

section 66A, etc, that talk about cybercrimes and upgrading the security of online exchange. The IT Act also gives the lawful structure to the online banking frauds and advancing the security and uprightness of electronic exchanges in India. Nevertheless, progressing improvements in innovation, advancing digital dangers, and arising administrative provokes require ceaseless updates and upgrades to India's legitimate and administrative system for online protection and electronic exchanges.[10]

The IT Act gives legitimate acknowledgment to electronic records and computerized marks, empowering the utilization of electronic reports and marks in online banking transactions. This works with the reception of advanced financial administrations while guaranteeing the legitimacy and enforceability of electronic agreements and exchanges. The IT Act characterizes different cybercrimes and offenses connected with unapproved access, hacking, information robbery, and deceitful exercises directed through electronic means, including online banking frauds. Offenses like unapproved admittance to PC frameworks, information modification, and the transmission of profane or hostile substances are culpable under the IT Act, with punishments going from fines to detainment.[11]

The IT Act also establishes the Cyber Appellate Tribunal (CAT)as an investigative position to hear requests against orders given by the Controller of Certifying Authorities (CCA) and settle matters connected with cybercrimes and electronic exchanges. The CAT has an essential role in mediating debates and implementing arrangements of the IT Act concerning online banking fraud. The IT Act engages the central government to assign capable specialists and administrative bodies to manage consistency with its arrangements and uphold guidelines connected with electronic exchanges, network safety, and information assurance.

4.2 Reserve Bank of India (RBI) Act 1934

The RBI issues rules and guidelines to banks and monetary organizations concerning network safety measures and misrepresentation anticipation. These rules incorporate prerequisites for carrying out safety efforts, detailing episodes of extortion, and client assurance measures. The Reserve Bank of India (RBI) assumes a focal part in managing and directing banks and monetary organizations in India, including their online financial transactions. While the

[10] The Information Technology Act, 2000
[11] Ibid at 4

Information Technology Act, of 2000 gives an expansive legitimate system to electronic exchanges and network safety, the RBI issues explicit guidelines and rules pointed toward shielding the trustworthiness of online financial administrations and safeguarding buyers from frauds and cybercrimes. [12]

The RBI has given far-reaching rules on network protection for banks and monetary foundations, including those offering online financial transactions. These rules frame the standards, norms, and best practices for overseeing digital dangers, carrying out strong safety efforts, and laying out compelling episode reaction systems to forestall and alleviate digital dangers, including online banking fraud. The RBI commands banks to lay out vigorous instruments for announcing and exploring online banking frauds and security occurrences speedily. Banks are expected to report huge cheats and security occurrences to the RBI and other important specialists speedily, attempt criminological examinations, and carry out medicinal measures to forestall repeat and relieve the effect on clients. Insurrection with RBI guidelines might bring about punishments, assents, or authorization activities against banks, accentuating the significance of adherence to administrative prerequisites in relieving online banking frauds.

4.3 Payment and Settlement Act of 2007

This act gives a legitimate structure to the guidelines and oversight of installment frameworks in India. It expects to guarantee the strength and effectiveness of installment frameworks and incorporates arrangements connected with electronic asset moves and online exchanges. This Act is a critical piece of regulation in India that oversees the guidelines and management of installment frameworks and settlement systems in the country. While it fundamentally centres around guaranteeing the productivity, security, and solidness of installment frameworks, the Act additionally contains arrangements pertinent to online banking frauds. The Act fills in as a basic official structure for controlling electronic installment frameworks and online banking transactions in India.[13] By advancing security, proficiency, and shopper assurance in installment frameworks, the Act adds to alleviating the dangers of online banking frauds and cultivating trust in the computerized installment environment. The PSS Act gives a legitimate

[12] Reserve Bank of India. (2025). *Official website*. Retrieved April 2, 2025, from https://website.rbi.org.in/en/web/rbi.
[13] The Payment and Settlement Act, 2007 https://ifsca.gov.in/Document/Legal/67-the-payment-and-settlement-systems-act-200712092020034236.pdf

structure to the guidelines and oversight of different installment frameworks working in India, including electronic funds transfer (EFT), card installments, portable installments, and financial transactions. It engages the Reserve Bank of India (RBI) to control and oversee instalment framework administrators, including banks and non-bank substances, to guarantee consistency with recommended norms and rules. [14]

Under the PSS Act, installment framework administrators are expected to carry out safety efforts and chance administration practices to safeguard against unapproved access, cheats, and digital dangers. The RBI issues rule on network protection, confirmation, encryption, and other security norms to relieve the dangers related to online financial transactions and improve the security of instalment frameworks. The PSS Act incorporates arrangements pointed toward defending the interests of shoppers utilizing electronic installment frameworks, including online banking administrations. It requires installment framework administrators to take measures for client verification, debate goal, objection redressal, and repayment of unapproved exchanges to shield buyers from online banking fraud and guarantee fair treatment.[15]

4.4 Prevention of Money Laundering Act (PMLA), 2002

The Prevention of Money Laundering Act (PMLA) plays a vital role in tackling online banking fraud by requiring financial institutions to implement strict anti-money laundering (AML) measures. These include enforcing Know Your Customer (KYC) protocols, closely tracking financial transactions, and swiftly reporting any suspicious activities to relevant authorities. Such proactive measures help disrupt fraudulent financial operations and enhance security within the banking sector. PMLA is designed to prevent the concealment of illegally acquired funds. It strengthens consumer protection by requiring financial institutions to conduct rigorous due diligence procedures. Financial institutions are responsible for scrutinizing transactions to detect any unusual or suspicious patterns that could indicate money laundering or financial misconduct. Under the PMLA, banks are required to keep detailed records of transactions and customer data, ensuring accountability and facilitating the detection of potential illegal activities. By enforcing anti-money laundering protocols, banks can weaken fraudulent financial networks and deter criminal activities by limiting their ability to operate undetected.

[14] Gabriel García Márquez, Home | Department of Economic Affairs | Ministry of Finance | ..., MAJOR FUNCTIONS. 2019. Available at: https://dea.gov.in/

[15] Reserve Bank of India. (2025). *Payment and Settlement Systems Act, 2007*. Retrieved, from https://www.rbi.org.in/SCRIPTs/OccasionalPublications.aspx?head=Payment%20and%20Settlement%20Systems%20Act,%202007.

The PMLA plays an indirect role in safeguarding online banking transactions by emphasizing the importance of strong cybersecurity measures to prevent unauthorized access and data breaches.

4.5 Know Your Customer (KYC) Norms

Know Your Customer (KYC) regulations play a crucial role in combating digital banking fraud by enforcing strict identification and monitoring procedures. Under these norms, banks must authenticate customer identities using official documentation and evaluate their risk profiles. This process helps prevent the creation of fraudulent accounts and illegal financial activities within the banking sector. KYC also facilitates continuous transaction monitoring, enabling banks to detect irregular patterns or suspicious activity. Institutions are required to report such incidents to the appropriate authorities while maintaining comprehensive records of customer details and financial transactions. Additionally, the integration of advanced technologies—such as biometric verification and real-time authentication—further strengthens KYC measures, enhancing security and reducing fraudulent activities in online banking.

4.6 Bharatiya Nyaya Sanhita 2023

The Bharatiya Nyaya Sanhita (BNS) 2023[16], which replaces the Indian Penal Code (IPC), introduces updated provisions for addressing various criminal offenses, including measures aimed at combating online banking fraud. This new legal framework marks significant progress in integrating digital forensics into India's judicial system. To fully leverage its potential, further advancements are needed in certain areas. Law enforcement officers, legal experts, and the general public must deepen their understanding of digital forensics and its role in legal proceedings. Strengthening collaboration between law enforcement agencies, businesses, and academic institutions is essential for fostering innovation, research, and skill development in this field.

Given the cross-border nature of cybercrimes, seamless global cooperation is vital for gathering evidence and prosecuting offenders effectively. Tackling these challenges will enable digital forensics to become a crucial tool in upholding justice in the digital age. The BNS takes a

[16] The Bhartiya Nyaya Sanhita, 2023 No. 45 of 2023

forward-thinking approach to criminal justice, positioning India as a leader in the integration of technology within law enforcement and the judicial system.

a. Cheating

Addressing numerous instances of fraud and cheating throughout India has been made possible in large part by SECTION 318(4)[17]. This section gives law enforcement organizations a strong tool to prosecute offenders in cases involving financial fraud, real estate scams, or online cheating. This provision covers fraudulent activities such as stealing passwords, developing fake websites, and committing various types of cyber frauds. The penalties, including imprisonment and fines, are determined based on the severity and impact of the offense.

b. Cyber Theft

Section 303 of the Bharatiya Nyaya Sanhitha addresses the theft of mobile devices, digital data, and computer hardware, providing a legal foundation for prosecuting cyber theft. However, when specific laws such as the Information Technology Act, 2000, apply, they take precedence over this section. This provision complements the IT Act by covering aspects not explicitly addressed within its scope, thereby strengthening legal protections against digital property theft. The Information Technology Act, 2000, primarily governs data theft in India. It prescribes penalties for unauthorized disclosure of information in violation of lawful contracts under Section 72A and for breaches of confidentiality and privacy under Section 72. If an individual unlawfully acquires or misuses confidential customer data - such as a client list - resulting in a privacy breach, they may be held accountable under Section 72 of the Act. This legal framework ensures comprehensive protection against cyber theft while maintaining justice for victims.

c. Possessing Stolen Property

Section 317 of the BNS 2023 addresses cases where individuals are found in possession of stolen items, including mobile phones, computers, and digital data. This provision is not restricted to the original offender but extends to anyone holding or possessing stolen property,

[17] 318 (4) Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

even if it has been transferred to a third party. The scope of Section 317 includes stolen digital assets such as mobile devices, computers, and electronic data. It applies to both the person responsible for the theft and any individual found in possession of these stolen items, whether they acquired them knowingly or unknowingly. The primary objective of this provision is to disrupt the cycle of criminal activity by ensuring accountability for all individuals involved in handling stolen digital property.

d. Making A False Document or False Electronic Record

Section 335 of the BNS, addresses offenses involving the fabrication, alteration, or transmission of fraudulent documents and electronic records with the intent to deceive or commit fraud. This provision penalizes acts of forgery, including the unauthorized use of electronic signatures and the exploitation of vulnerable individuals. The primary objective of this section is to safeguard the authenticity and reliability of both physical and digital records. By imposing strict legal consequences on those engaged in document falsification, it reinforces trust in official documentation and prevents fraudulent practices.

Under the section an individual is considered to have committed an offense if they create, sign, or affix a seal to a document or a portion of it with dishonest or fraudulent intent. This also includes generating unauthorized electronic records or transmitting them without proper authorization. The primary goal behind such actions is to deceive others into accepting the document as genuine. Under Section 335 of the BNS, the scope of forgery extends to digital activities, including the unauthorized use of electronic signatures on electronic records. The concept of affixing an electronic signature is governed by the provisions of the Information Technology Act, 2000. Fraudulent activities, such as unauthorized electronic signing of emails or documents, fall under the category of digital forgery.

This legal measure is intended to uphold the security and authenticity of digital transactions, contracts, and communications, ensuring they receive the same level of protection as physical documents. By enforcing strict regulations, it helps prevent misuse and reinforces trust in electronic documentation.

e) Cyberstalking

Section 78 of the BNS, plays a vital role in addressing cyberstalking, imposing penalties for

both physical and online stalking. This provision recognizes the emotional and psychological harm caused by such actions and aims to deter offenders through legal consequences. By criminalizing cyberstalking, the law seeks to create a safer digital environment, with a particular emphasis on protecting vulnerable individuals, including women and children. The enforcement of this section strengthens legal safeguards against harassment, ensuring accountability for those who engage in such behaviour.

f) Dishonest Misappropriation of Property

Section 314 of the BNS addresses cases where individuals gain unauthorized access to computer systems or networks and unlawfully acquire or use digital data for personal gain. Although digital data is intangible, it is legally recognized as movable property and is considered misappropriated when taken without the rightful owner's consent, whether an individual or a business entity. Hackers may exploit this data for fraudulent activities, personal advantage, or to cause harm. Such actions fall under dishonest misappropriation, as they involve the unauthorized acquisition and use of another party’s digital assets for unlawful benefit. This provision ensures accountability for cyber offenses and reinforces legal safeguards against digital property theft.

g) Cheating by Personation

Section 319 of the BNS addresses cases where an individual deceives another into transferring property or providing valuable security through dishonest means. This provision specifically covers cheating by personation, which occurs when someone falsely assumes another’s identity, knowingly substitutes one person for another, or misrepresents themselves or someone else. The law recognizes such fraudulent actions as serious offenses, ensuring accountability for individuals who engage in deception for personal gain. By penalizing impersonation-based cheating, this section reinforces legal safeguards against fraudulent transactions and identity misuse.

5. Role of Technology in Combating Digital Banking Frauds

Digital banking has become the preferred method for consumers to manage financial tasks, including account management, bill payments, and transactions. While these services offer convenience, they have also created opportunities for fraudsters to exploit online systems. The

rise of faster payment systems has reshaped fraud tactics. Previously, cybercriminals primarily targeted banking infrastructure, but now they focus on deceiving users directly. This shift presents new challenges for fraud prevention teams, increasing financial risks. The immediacy of digital payments, coupled with outdated security technologies, makes it difficult to detect fraudsters who bypass direct interaction with banking platforms.

To counter these threats, financial institutions are integrating advanced security technologies. AI-driven algorithms analyze transaction patterns to identify anomalies, helping banks detect and prevent fraudulent activities. Technological advancements have significantly influenced banking fraud in India, both positively and negatively. On the one hand, innovations such as artificial intelligence (AI), machine learning (ML), biometric authentication, and blockchain have enhanced security measures. On the other hand, evolving fraud techniques continue to challenge financial security. This ensures stronger fraud detection capabilities while reinforcing trust in digital banking.[18]

AI-driven algorithms possess the ability to process large volumes of transaction data in real-time, enabling the detection of unusual patterns that may signal fraudulent activities. Biometric verification technologies, including fingerprint scanning and facial recognition, have strengthened identity validation, significantly reducing unauthorized access and identity fraud. However, technological advancements have also introduced new vulnerabilities that cybercriminals can exploit. Sophisticated phishing techniques, malware, ransomware, and social engineering tactics have evolved, targeting individuals and organizations through emails, social media, and digital platforms. AI-driven algorithms analyze vast amounts of transaction data in real-time, identifying irregular patterns and detecting potentially fraudulent activities. Machine learning models effectively distinguish between legitimate and fraudulent transactions, enabling banks to take proactive measures to mitigate risks and prevent financial losses. Additionally, AI-powered chatbots and virtual assistants enhance customer interactions by providing real-time assistance, reducing the likelihood of users falling victim to phishing schemes or social engineering attacks.[19]

[18] BioCatch. (2023, September 18). BioCatch Connect: Reshaping How Fraud and AML Teams Work Together. https://www.biocatch.com[](https://www.prnewswire.com/news-releases/biocatch-scout-delivers-financial-pre-crime-logistical-intelligence-for-targeted-fraud-interdiction--mule-account-identification-301929903.html)
[19] Ibid

Despite the benefits of AI and ML in fraud prevention, challenges remain, including concerns over data privacy, biases in algorithms, and the complexity of understanding how these models operate. Addressing these issues is crucial to ensuring the ethical and responsible implementation of these technologies in financial security.

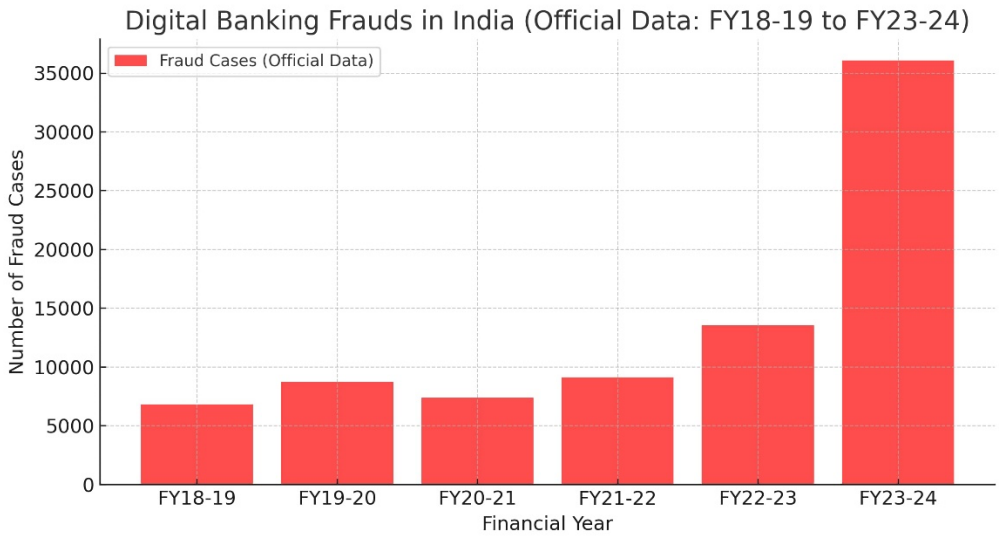

FIGURE 2: Figure derived from the compilation of Reserve Bank of India Annual Report.

This figure shows the compilation of all the Reserve Bank of India report, showing the number of digital banking fraud cases in India from the FY2018 – 2019 to FY2023 – 24. This data indicates a significant surge in the number of digital banking frauds in the last two fiscal years. The figures above represent the total number of reported fraud cases in the banking sector, with a substantial portion attributed to digital payment channels, including card and internet banking frauds. For instance, in FY2022 – 2023, nearly 49% of the total fraud cases were related to digital payments.[20]

[20] The Indian Express. (2023, May 30). Banks saw highest number of frauds in digital payments in FY23: RBI. https://indianexpress.com/article/business/banking-and-finance/digital-payment-frauds-in-fy23-rbi-report-8637607/[](https://indianexpress.com/article/business/banking-and-finance/digital-payment-frauds-in-fy23-rbi-report-8637607/)

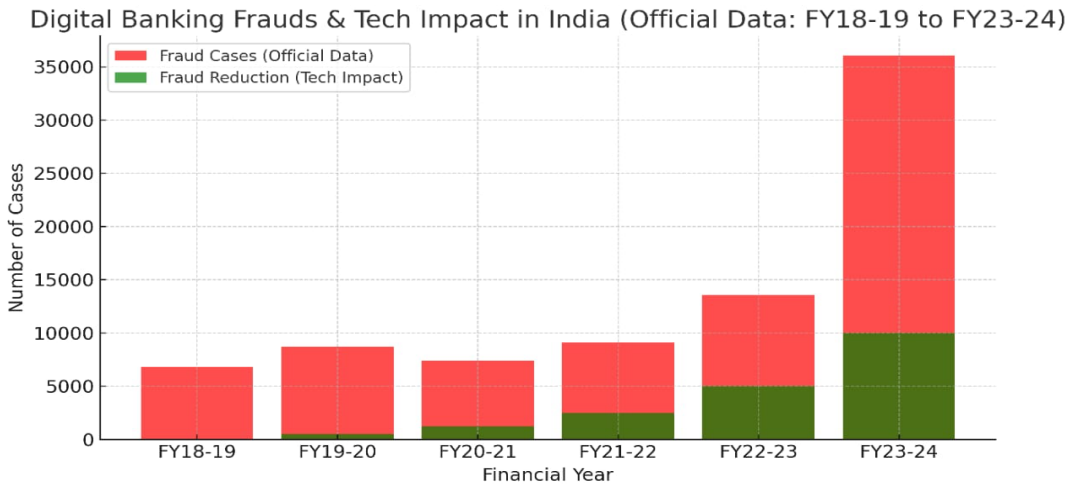

FIGURE 3: Figure derived from the compilation of Reserve Bank of India Annual Report with a hypothetical addition of technology in curbing Digital Banking Frauds.

The official data from the Reserve Bank of India (RBI) highlights the number of digital banking fraud cases in India from FY2018–19 to FY2023–24. This data also reflects the role of technological advancements in reducing fraud incidents over time. Since FY2019–20, security technologies such as AI-powered fraud detection, real-time transaction monitoring, biometric authentication, and blockchain have contributed to a decline in fraud cases. By FY2023–24, these innovations are estimated to have prevented approximately 10,000 fraud incidents, demonstrating their effectiveness in enhancing financial security[21]

6. Indian Judiciary on Online Banking Frauds

a. Punjab National Bank Fraud (Nirav Modi Case)

One of the biggest banking scams in India was the Punjab National Bank (PNB) affair, which was made public in 2018. It involved about $1.8 billion (₹14,000 crore). In cooperation with some PNB officials, Nirav Modi and his uncle Mehul Choksi, proprietors of high-end jewellery brands, planned the scam. The illegal issuance of Letters of Undertaking (LOUs), which are bank guarantees that enable businesses to raise money from foreign banks, was at the centre of the scam. Based on fictitious LOUs issued by PNB's Brady House branch in Mumbai, Modi's companies were able to obtain loans from overseas branches of Indian Banks without having

[21]Figure 3 is a hypothetical graph derived to depict the role of technology in mitigating digital banking frauds

to provide the required collateral. [22]

As PNB's Core Banking System (CBS) was not integrated with the SWIFT (Society for Worldwide Interbank Financial Telecommunications) network, which enabled these unauthorised transactions, the fraud was undiscovered for several years. In January 2018, PNB officials discovered inconsistencies in their records, which led to the discovery of the scam. The Enforcement Directorate (ED) and Central Bureau of Investigation (CBI) then began their investigations, which resulted in several arrests and asset seizures. Owing to the exposure of significant weaknesses in internal control and banking, the Reserve Bank of India (RBI) strengthened trade finance laws after this scam. This case highlighted systemic issues in India's banking sector, including weak risk management practices and lack of oversight.

b. The Yes Bank Phishing Scam (India, 2021)

In the year 2021, Securities and Exchange Board of India (SEBI) scrutinised YES bank for fraudulent realisation of Additional Tier-1 (AT1) Bonds. A penalty of ₹250 million was imposed on Yes Bank, declaring that the bank had misguided the retail investors to invest on these high-risk bonds as low- risk investments including senior citizens, without disclosing the risks associated with these investments. [23]This misrepresentation resulted in significant financial losses for several investors when the bank used these bonds to stabilize their financial position. In addition to this, Yes Bank has cautioned its customers regarding voice phishing scams, where fraudsters impersonate bank officials over the phone to obtain financial and personal details.

c. The Rise of UPI-Based Phishing Scams in India

The Unified Payments Interface (UPI) has revolutionized digital banking in India by facilitating instant financial transactions. However, with its rapid usage, deceivers have adopted advanced techniques to exploit customers. Phishing attempts, which target people through fake UPI links and fraudulent customer support calls, are the most common scams. For instance, Mr. Rajesh Sharma, a working professional stationed in Mumbai, received a call from a person claiming to be a bank official. The fraudster informed him that his KYC (Know

[22] The Panjab National Bank Limited vs The Mercantile Bank of India Limited on 9 March, 1911
Equivalent citations: (1911)13BOMLR835, 12IND. CAS.257
[23] Mehta, A. (2024). Impact of technological advancements on banking frauds: A case study of Indian banks. International Journal of Research in Finance and Management, 7(1), 261–266.

Your Customer) information required to be update immediately to prevent account cancellation. The caller sent a UPI collect request and directed Rajesh to approve it, stating it was a verification step. Trusting the caller, Rajesh approved the request link, unknowingly transferring ₹50,000 from his bank account.

d. The Cosmos Bank Cyber-attack (2018):

Cosmos Bank, a Cooperative Bank with its headquarters in Pune, suffered a sophisticated cyberattack in August 2018 that costs ₹94 crore. Through malware, hackers were able to access the bank's SWIFT (Society for Worldwide Interbank Financial Telecommunications) network by intruding its internal systems. Cybercriminals used cloned debit cards to withdraw substantial amounts of money over the period of 2 days from ATMs in 28 different countries. Additionally, fraudulent SWIFT transactions were used to transfer ₹13.92 crore to a Hong Kong bank. Banks throughout India tightened their transaction monitoring procedures strengthened their cybersecurity frameworks in the wake of the incident to avoid similar attacks in the future.[24]

7. Conclusion and Suggestion

In today's digital era, raising awareness and educating the public about financial fraud is essential to protecting banking customers from online threats. Banks play a crucial role in protecting consumers by implementing secure practices and promoting awareness. To mitigate fraud risks, financial institutions should regularly communicate security updates via SMS, email, and social media, educating customers about emerging cyber threats. Customers must be advised never to share sensitive information such as OTPs, passwords, or PINs, as legitimate banks do not request such details. Additionally, users should ensure they download banking applications only from trusted sources like the Google Play Store or Apple App Store. Enhancing security measures involves encouraging customers to activate two-factor authentication and transaction alerts, enabling real-time monitoring of account activity. Users should also remain vigilant against suspicious links received through email, SMS, or WhatsApp to prevent phishing attempts.

[24] Mehta, A. (2024). Impact of technological advancements on banking frauds: A case study of Indian banks. International Journal of Research in Finance and Management, 7(1), 261–266.

By promoting responsible digital practices, banks can significantly reduce fraud cases and strengthen customer trust. A secure digital banking ecosystem requires collaboration among regulatory authorities, financial institutions, and consumers to ensure a safer and more reliable financial system. To sum up, disseminating knowledge and raising awareness on digital fraud is essential to protect the interests of banking clients in this modern world. To safeguard consumers from online dangers, Banks must be proactive in educating the public, running awareness programs, and implementing secure banking practices. Financial institutions may drastically lower fraud incidents and increase consumer trust by encouraging vigilant and responsible digital behaviour. A collaborative effort between regulatory authorities, banks, and customers is essential to build a safer digital banking environment.

References:

1.) Kaur, P., & Sharma, R. (2021). The rise of digital banking frauds: Trends, challenges, and preventive measures. Journal of Financial Crime, 28(4), 123-145.

2.) Singh, A., & Jain, R. (2023). Artificial intelligence in banking fraud detection: Opportunities and risks. Cybersecurity Review, 15(2), 87-102.

3.) Smith, J. (2023). Cybercrime in the digital banking era: Prevention and risk management. Oxford University Press.

4.) Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A systematic literature review of e-banking frauds: Current scenario and security techniques. Linguistica Antverpiensia, 2021(2), 3509–3517.

5.) Mehta, A. (2024). Impact of technological advancements on banking frauds: A case study of Indian banks. International Journal of Research in Finance and Management, 7(1), 261–266.

6.) Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain South African Journal of Information Management, 26(1), a1763.

7.) Reurink, A. (2018). Financial fraud: A literature review. Journal of Economic Surveys, 32(5), 1292–1325

8.) **ICLG.** (2025). *Cybersecurity Laws and Regulations Report 2025 India*. ICLG

9.) Johann Wolfgang von Goethe, Information technology act, 2000, Information Technology Act,2000.2019https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

10.) BioCatch. (2023, September 18). BioCatch Connect: Reshaping How Fraud and AML Teams Work Together. https://www.biocatch.com[](https://www.prnewswire.com/news-releases/biocatch-scout-delivers-financial-pre-crime-logistical-intelligence-for-targeted-fraud-interdiction--mule-account-identification-301929903.html)

11.) Ainsley Granville, Andre Jorge Bernard, Brahma Edwin Barreto, Rodney D'Silva. 2019.

"Impact of Frauds on the Indian Banking Sector." 8 (7S2): 219-223

12.) Haugen, S. and Roger Selin, J. 1999. "Identifying and controlling computer crime and employee fraud." Industrial Management & Data Systems, 99 (8): 340-344

13.) Singh, Parisha. (2018). Online Banking Frauds and Role of Government to Curb It: With

Special Reference to India. Supremo Amicus, 3, 365-375

14.) D.K. MURTHY, VENUGOPAL, INDIAN BANKING SYSTEM (IK International Publishing House Pvt. Ltd., 2006) 10-20.

15.) V. Rajendran, Banking on IT's Security, JOURNAL OF INDIAN INSTITUTE OF BANKING AND FINANCE, 2018