INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

A COMPREHENSIVE ANALYSIS OF BANKING FRAUD AND REGULATORY RESPONSES IN INDIA.

AUTHORED BY - JENNIFER NENGNEIVAH HAOKIP & MUSKAN JAJOO

1. INTRODUCTION

"Fraud and deceit are anxious for your money. Be informed and prudent."

— John Andreas Widtsoe

Indian Banking sector over the recent years has witnessed a drastic change with the rapid development of digital inventories. While digital transformation along with financial sector reforms, change in regulation, global competitiveness and evolving strategies of banks has undoubtedly made our lives much efficient and convenient, with the growing usage it has also opened new avenues for fraudulent activities.

Fraudsters are continuously evolving their tactics, moving from traditional skimming to more advanced forms of social engineering, like vishing and smishing, that exploit a user's trust and lack of digital literacy. The sheer volume of digital fraud cases, though often of lower value compared to large-scale loan frauds, poses a significant threat to consumer confidence and the integrity of the financial ecosystem with the Reserve Bank of India (RBI) reporting a surge in the number of cases and a substantial increase in the value of digital-payment-related frauds.[1] The proliferation of UPI and other instant payment systems, while facilitating seamless transactions, has also introduced new avenues for fraudsters, with scams involving fake payment requests and fraudulent QR codes becoming commonplace. The challenge is compounded by the persistent lag in fraud detection and the low digital literacy among a large segment of the Indian population, making them susceptible targets.[2]

[1] Reserve Bank of India, *Annual Report 2023-24* 110 (2024),https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1214.
[2] Rahi Bhattacharjee, *RBI Annual Report FY24: What caught our attention?*, BUREAU (June 1, 2025), https://bureau.id/resources/blog/rbi-annual-report-fy24-what-caught-our-attention/.

ISSN: 2582-6433

2. REVIEW OF LITERATURE

2.1."Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance"[3]

This paper provides a detailed analysis of the evolving landscape of digital banking frauds in India, moving beyond traditional methods to focus on new-age scams enabled by social engineering. It classifies frauds into distinct typologies, such as phishing, UPI-related scams, and SIM swaps, highlighting how these schemes prey on user behaviour and lack of digital literacy. The authors argue that traditional rule-based fraud detection systems are no longer adequate. They propose a shift towards AI-enabled risk governance, which uses machine learning to analyse behavioural biometrics and transaction patterns to predict and prevent fraud in real-time. The paper concludes with a framework for a multi-layered defence strategy, emphasizing a balance between technological safeguards and consumer education to build a more resilient financial ecosystem.

2.2.Gupta, S. (2023). Electronic Banking Frauds: The Case of India[4]

This paper examines the emergence of electronic banking frauds in India, which has brought a shift in high pace expanding digital banking services. It emphasizes the need for effective fraud detection mechanisms and regulatory frameworks to regulate and safeguard financial transactions. Ebanking in India has led to an increase in cybercrimes, with fraudsters exploiting technological vulnerabilities. Previous research indicates that while digital banking offers convenience, it also exposes users to risks such as phishing, identity theft, and unauthorized transactions. Studies suggest that a combination of advanced technology and stringent regulations is essential to combat these frauds effectively. Furthermore, educating consumers about safe online banking practices has been identified as a critical component in reducing fraud incidents.

2.3.Frauds in the Indian Banking Industry: An Analysis.[5]

This research provides a comprehensive outline of the scenario in the Indian banking sector. It analyzes trends from official RBI data, revealing a concerning rise in the volume and value of

[3] Maini, R., & Sindhi, V. K. (2025). Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance. *International Journal of Finance and Management Research*, 7(5). DOI: 10.36948/ijfmr.2025.v07i05.55593

[4]Gupta, S. (2023). Electronic Banking Frauds: The Case of India. In *Electronic Banking Frauds: The Case of India* (pp. 166-180). IGI Global

[5]Indian Institute of Management Bangalore. (2024). *Frauds in the Indian Banking Industry: An Analysis*. IIMB Working Paper No. 505. Retrieved from https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf

ISSN: 2582-6433

frauds, with a notable shift from large-scale corporate loan frauds to a high frequency of digital, retail-level scams. The paper attributes this surge to key vulnerabilities, including weak cybersecurity protocols at some financial institutions and a lack of standardized, real-time fraud reporting. It critically evaluates existing regulatory frameworks and highlights their limitations in keeping pace with rapidly evolving cyber threats. The authors call for stronger regulatory oversight, urging for a collaborative fraud intelligence-sharing platform and mandatory adoption of advanced technological solutions to curb the menace.

3. RESEARCH DESIGN

The study uses a descriptive-analytical design with a doctrinal approach, examining laws, case law, reports, and data on digital banking frauds in India. Through qualitative and comparative analysis, it identifies vulnerabilities, assesses regulatory responses, and proposes multi-stakeholder strategies to enhance fraud prevention and strengthen financial security.

4. CONCEPT, DEFINITION, NEED FOR COMBATING BANNKING FRAUDS

4.1. CONCEPT OF BANKING FRAUD

Fraud in simple terms can be defined as deceit, trickery or deception done willfully by a person. Fraudulent activities is not a novice concept and has been going on since time immemorial. Physical banks have also witnessed various classifications of frauds such as Criminal breach of Trust, Misappropriation, Manipulation of books, Fraudulent activities by forged instruments, cheating, forgery, unauthorized transactions etc. Coming on to the digital era, these forms of frauds still persist. Although technological advances have provided convenience to consumers in the digital era, it's not without a drawback, new methods of frauds have also been introduced such as phishing, identity theft, pharming and other e-frauds technological advancement leads to difficulties in recognizing and investigating.

4.2.DEFINITIONS: FRAUD, BANKING FRAUD

- **S.17 of Contract Act, 1872** defines fraud as an act done by a party to a contract or by his agent or connivance with an intent to deceive or induce a person into entering into contract. It includes: (i) Suggesting a fact that is not true, by someone who doesn't believe it to be true (ii) actively concealing a by someone who has knowledge or belief of fact (iii) Making a promise with no intention of fulfilling it.(iv) Any other action

ISSN: 2582-6433

intended to deceive.(v) Any act or omission that the law specifically designates as fraudulent.

- **RBI, the regulator of banks in India**, defines fraud as "Any act of omission or commission of any person in a banking transaction, or in the books of accounts kept by banks by hand or under computer system, which causes a temporary or other wrongful gain to any person and or without any loss to the bank.".
- **Bank fraud** is a crime that is committed in the context in which an individual employs unlawful methods in obtaining money or other assets in a financial institution or bank. It also denotes the efforts of an individual in order to secure the funds of the depositors of the bank by pretending to be a bank or any other financial organization.

5. NEED FOR COMBANTING FRAUD IN DIGITAL ERA

Combating banking fraud in the digital era is imperative due to the escalating sophistication of cyber threats and their profound impact on individuals and financial institutions. The surge in digital banking has expanded the attack surface for fraudsters, leading to increased incidents of online fraud. Advanced technologies like artificial intelligence (AI) have empowered fraudsters to devise more intricate schemes, making traditional detection methods less effective.

Such frauds not only result in significant financial losses for individuals and institutions but also damage public trust in the banking system. Additionally, regulatory bodies impose strict compliance standards on banks, and failure to prevent fraud can lead to legal and reputational consequences.[6]Combating banking fraud is therefore essential to safeguard customer assets, maintain confidence in digital financial services, ensure regulatory compliance, and promote the overall stability of the financial system in a highly interconnected and technologically driven economy.

6. TYPES OF FRAUDS IN BANKING:

6.1.PHISHING

It is one of the most common methods of ebanking fraud. Here the fraudsters pretend to be bankers themselves, and then float a site that is similar to the persons bank and through this

[6] Arushi Mehta, Impact of technological advancements on banking frauds: A case study of Indian banks, IJRFM, Vol 7(1), 261-266 (2024)

ISSN: 2582-6433

method obtain the personal details of customers.[7] Fraudsters often deceive customers into sharing personal and account details under the pretext of updating bank's records. On receiving sensitive information such as usernames, passwords and card details, they conduct unauthorized transactions without the knowledge of victim.[8]

6.2.SPAM

Usually, in this method fraudsters send 'junk mail' or unwanted messages in the form of mail or sms which is often disguised as promotional offers. Customers are often persuaded to buy a product or service or even visit a website on being provided a link where purchases can be made and are thus tricked into giving away bank account or credit card details. These messages can lead to websites wherein financial credentials are retrieved for fraudulent purposes.[9]

6.3.HACKING

It involves illegal entry into a system. Mobile banking apps though comparatively safer than browsers are not immune to fraud, money laundering and cybercrime.[10]

6.4.STOLEN CVV AND OTP SCAMS:

Fraudster contacts the victim under the pretext of purchasing a product or service. Claiming to make an advance payment as confirmation, the fraudster requests details related to digital wallet or payment gateway.[11] Then ask for OPT sent to victim's phone. Once the OTP is shared the fraudster gains access to victims account an may initiate multiple unauthorized transactions, usually unnoticed by the victims.

6.5.VISHING

It happens when scammers makes phone calls or VoIP (Voice over Internet Protocols) disguising themselves as a legitimate person or organisation in order to gain the victim's trust by asking for sensitive information such as passwords or credit number and using certain to

[7] Reserve Bank of India, *Report on Trends and Progress of Banking in India* 85 (2023), https://www.rbi.org.in (last visited Sept. 15, 2025).
[8] Press Information Bureau, Ministry of Electronics & Information Technology, *Phishing Attacks on Digital Payment Users Rise in India*, https://pib.gov.in (last visited Sept. 16, 2025)
[9] Reserve Bank of India, *Cyber Security Framework in Banks* (2016), https://www.rbi.org.in, (last visited Sept. 16, 2025)
[10] KPMG, *Fraud Survey: Navigating the New Age of Cybercrime in Indian Banking* 34 (2022), https://kpmg.com (last visited Sept. 15, 2025)
[11] PwC India, *Fraud in the Digital Age: India Banking Sector Survey* 58 (2022), available at https://www.pwc.in (last visited Sept. 19, 2025)

ISSN: 2582-6433

inculcate fear or urgency.

6.6.SKIMMING

There are three different forms of skimming:

(a) Card skimming- It refers to the illegal duplication and collection of information stored on magnetic stripe and PIN data on credit and debit cards. It can occur at any ATM or through tampered EFTPOS (Electronic Funds Transfer at Point of Sale) terminal.[12] Here the data collected is encoded on counterfeit cards which is used to withdraw money or carry out fraudulent transactions.

(b) ATM skimming: Fraudsters install fake pin pad covers or card reader overlays onto ATMs. They also attach disguised skimming devices to card slots, paired with hidden cameras to record users entering their PINs which allows them to steal card data and PIN information.

(c) EFTPOS skimming: it happens when foreign device is embedded into point of sale terminal. This device captures card details and PINS during legitimate transactions. Tampering internal therefore detecting compromised EFTPOS machine requires close physical inspection.[13]

6.7. IDENTITY THEFT

Criminals and fraudsters steal identity of victims by attaining personal information such as PAN numbers, Adhaar details or bank credentials, through computers whereby fake bank accounts and are set up and loans taken under customers under names to perpetuate cybercrimes.[14]

7. LEGAL FRAMEWORK REGULATING BANKING IN INDIA

7.1.THE BANKING REGULATION ACT, 1949[15]:

Although the act does not directly address frauds in banking, the provisions provided under the act help in understanding the regulations and procedure of banking industry to a certain extent, thus providing an insight as to what factors contribute to banking frauds.

[12] Indian Cyber Crime Coordination Centre (I4C), *Card Skimming Threat Landscape in India* 21 (2023), available at https://www.mha.gov.in (last visited Sept. 19, 2025)
[13] Indian Computer Emergency Response Team, *EFTPOS Fraud: Detection and Mitigation Guidelines* 13 (2021), available at https://www.cert-in.org.in (last visited Sept. 20, 2025)
[14] Ministry of Home Affairs, *Annual Report on Cyber Crime in India* 102 (2023), available at https://www.cert-in.org.in, (last visited Sept. 20, 2025)
[15] The Banking Regulation Act, No. 10 of 1949

ISSN: 2582-6433

7.2.INFORMATION TECHNOLOGY ACT, 2000[16]:

This act governs various aspects of ecommerce and cybercrime and addresses cybercrtimes through sections 46 and 66A. It provides regulations relating to hacking, data theft and online fraud. It also supports digital business operations, facilitate the use of digital signatures and legally recognize electronic transactions. In addition, the Act provides the legal structure to the ebanking frauds and enhances the security of electronic exchanges in India.[17]

7.3.THE RESERVE BANK OF INDIA ACT, 1934[18]:

The RBI plays crucial role in regulating and supervising banks and financial institutions, especially in relation to cyber security and fraud prevention issues guidelines and rules to administer online financial transactions and safeguards buyers from fraud and cybrcrime. These rules provide the norms and standards to manage cyber threats, implementing security protocols.

The RBI also performs regular audits and inspections of banks' digital operations to ensure compliance. Failure to follow these regulations can lead to penalties, reinforcing the need for strong cyber security and fraud management systems.

7.4.PAYMENT AND SETTLEMENT SYSTEMS ACT, 2007[19]

The Act provides framework to ensure secure, efficient and stable digital transactions including fund transfers EFT, card payments and mobile banking. RBI controls and regulates bank and non bank payment system to adopt robust security and risk management practices to protect against cyber threats and unauthorized access. According to the Act, the administrators are required safety measures to safeguard against unverified access, cheats, and electronic threats. The RBI provides guidelines for network protection, confirmation, encryption, and other security norms.[20]

8. JUDICIAL DECISIONS

8.1.SONY-SAMBANDH CASE (2002)[21]

This was one of the first case in relation to online related fraud case in India. This case is a

[16] The Information Technology Act, No. 21 of 2000
[17]Mrs. Ramya& Suresh Mathew Raj G,Laws Regulating Online Banking Frauds in India: A Comparative Study with Existing Laws in USA, Vol XIV, AARJ,3-4(2024), 1-AUT-MAY-2024-4704.pdf
[18] The Reserve Bank of India Act, No. 2 of 1934
[19] The Payment and Settlement Systems Act, 2007, No. 51 of 2007, Acts of Parliament, India
[20]Ibid at 7
[21]Sessions Case No. 27/2003, Special Judge, Tis Hazari Court, Delhi

ISSN: 2582-6433

testimony that in situations where IT Act does have provision relating to certain category cybercrimes the Indian Penal Code can be applied in an effective manner. The complainant in this case was running a website wherein Nonresidents residing outside India can send Sony products to their Indian friends and relatives by making online payments.

On May 2022, through the identity of Ms.Barbara Campa an order was initiated containing a Sony TV set and cordless headphone where her credit card details were given for payment which was accepted by Sony India Ltd who later deliver the product to Arif Azim. Whereby the due diligence was followed and digital photo was also taken as evidence of the product being accepted by Arif Azim. After one month post transaction, Sony Company was informed that there was unauthorized fraudulent transaction as Mrs. Barbara denied making the transaction.

The company thereupon lodged a complaint for online cheating to CBI and Arif was found guilty and convicted by court under Sections 418, 419 and 420 of IPC for the offence of cyber fraud and cheating.

8.2.ICICI BANK PHISHING CASE[22]

The hazardous nature of emails to security was discovered in this case. In 2007-08, an NRI customer of ICICI Bank was defrauded via a phishing email that appeared to be from ICICI, asking him to reply with his internet banking user ID and password, under threat that his account would become "non-existent." After submitting the credentials, he later discovered that Rs 6.46 lakh had been transferred from his account to that of a company; of that amount, Rs 4.6 lakh was withdrawn at an ICICI branch in Mumbai. The customer filed a petition under the Information Technology Act, arguing the bank was negligent. ICICI's defence was that the customer "negligently disclosed" confidential information. The adjudicating authority directed the bank to pay Rs 13 lakh to the victim to cover financial loss, travel expenses, and other damages, finding in favour of the complainant due to lack of sufficient safeguards on the bank's part.

8.3.COSMOS BANK CYBER HEIST

This case was a malware attack committed between payment gateways which amounted to Rs. 78 crores withdrawn physically through 12,000 ATM outside India, while 2800 transactions were made in different corners of the country worth 2.5 crores by cloning thousands of debits

[22]ICICI Bank Ltd. v. Umakanta Mohapatra, (2009) 2 Comp LJ 199 (DRAT).

ISSN: 2582-6433

cards. This indicated ATMs releasing money regardless of whether the bank account existed or not. This incident exposed severe vulnerabilities in payment authorisation, transaction monitoring and interbank settlement systems, drawing regulatory scrutinity under India's payment framework.

9. EFFECTIVE STRATEGIES IN COMBATING DIGITAL FRAUDS AND ENHANCING CUSTOMER SAFETY

9.1. Artificial Intelligence and Machine Learning

AI and ML algorithms are at the forefront of fraud detection. These systems analyze vast amounts of transaction data to identify anomalies and suspicious patterns that would be impossible for a human to spot. They can monitor for behaviours like unusually high-value transactions, transactions from new locations or devices, or a sudden change in spending habits. The Reserve Bank of India (RBI) has even launched initiatives like MuleHunter.AI to leverage AI and ML against mule accounts.[23]

9.2.Behavioural Biometrics:

This technology goes beyond traditional authentication methods like passwords and OTPs. It analyzes a user's unique digital footprint, including keystroke dynamics, mouse movements, and how they navigate an app.[24] In case any fraudster gains access to a user's credentials, behavioural biometrics can detect that the user's behavior is inconsistent with their established pattern, flagging the transaction for further review.

9.3.Device Intelligence:

This technology uniquely identifies a device based on its hardware and software characteristics. It can help detect if an account is being accessed from a new or unfamiliar device, which is a common indicator of account takeover fraud

9.4.Consumer Education and Awareness:

This is arguably the most critical non-technological strategy. Fraudsters primarily use social

[23]Shashank Survase,*Strategic Approaches for Combating Digital Financial Fraud in 2025*,https://bankiq.co/effective-strategies-to-mitigate-digital-financial-frauds-in-2025, (last visited 21.09.2025)
[24]M. S. Singh & P. K. Saxena, *How Technology Can Redefine Fraud Detection in Indian Banking Sector*, https://etedge-insights.com/technology/cyber-security/how-technology-can-redefine-fraud-detection-in-indian-banking-sector/(last visited 19.09.2025)

ISSN: 2582-6433

engineering tactics like phishing, vishing, and smishing to trick victims.[25] Financial institutions must conduct continuous, multi-lingual public awareness campaigns to educate consumers on:

- **Never sharing sensitive information** like OTPs, UPI PINs, or CVV.
- **Recognizing scam tactics** like urgent requests for money or lottery promises.
- **Verifying requests** by contacting the bank through official channels only.

9.5.Strengthening Regulatory Framework

The RBI plays a pivotal role in shaping the fraud prevention landscape. Stricter guidelines for payment aggregators, mandatory dispute resolution policies, and the establishment of a real-time fraud intelligence-sharing platform are vital. The RBI's push for a Digital Payment Intelligence Platform (DPIP) is a move in this direction, encouraging a collaborative ecosystem for fraud data sharing.[26]

9.6.Internal Controls and Employee Training

Banks must also focus on internal threats. Robust internal audits, segregation of duties, and regular training for employees on fraud prevention and detection are essential. Employees should be empowered to report suspicious activities without fear of retaliation.[27]

9.7.Customer-Centric Banking Practices

Banks can enhance consumer safety by offering services that enable customers to manage their own risk. For example, some banks now offer the ability for customers to set daily transaction limits or "sleep mode" on their accounts to temporarily disable transactions when not in use, a practice recently adopted by Airtel Payments Bank.[28]

10.FINDINGS OF THE STUDY

- Rapid digitalization has increased banking fraud risks, especially phishing, SIM swaps, and social engineering.

---

[25] A. K. Jain, *Cyber Security Tips*, UNION BANK OF INDIA, https://www.unionbankofindia.co.in/en/common/cyber-security, (last visited 21.09.2025)

[26] P. T. I., *RBI Issues Revised Guidelines for Payment Aggregators to Enhance Consumer Protection*, NEWS ON AIR (Sept. 17, 2025), https://www.newsonair.gov.in/rbi-issues-revised-guidelines-for-payment-aggregators-to-enhance-consumer-protection/.

[27] S. G. Pande, *Powerful Strategies to Combat Banking Frauds in India*, Indiaforensic, https://indiaforensic.com/powerful-strategies-to-combat-banking-frauds-in-india/.(last visited 21.09.2025)

[28] A. K. Jha, *Airtel Payments Bank launches 'safe second Account' to boost secure digital transactions*, TIMES OF INDIA, https://timesofindia.indiatimes.com/technology/tech-news/airtel-payments-bank-launches-safe-second-account-to-boost-secure-digital-transactions/articleshow/124053118.cms(last visited 15 Sept 2025)

ISSN: 2582-6433

- Existing legal and regulatory frameworks are inadequate to address evolving cyber threats.
- Weak internal controls, limited consumer awareness, and poor information sharing contribute significantly to vulnerabilities.
- Advanced technologies like AI can enhance fraud detection but require stronger implementation.
- A collaborative approach among regulators, banks, and consumers is crucial for effective prevention.

11.CONCLUSION

The proliferation of digital banking frauds in India presents a formidable challenge to the nation's financial stability and consumer trust. While the digital revolution has unlocked immense convenience, it has also exposed critical vulnerabilities that fraudsters are exploiting with increasing sophistication. The trends show a clear shift from large-scale corporate frauds to a high-volume, tech-enabled onslaught of retail scams, largely driven by social engineering. Effectively combating this menace requires a comprehensive and collaborative strategy. First, banks must move beyond traditional security measures and adopt **advanced technological solutions** like AI/ML-based anomaly detection and behavioral biometrics to predict and prevent fraudulent activities in real-time. Second, a **proactive regulatory framework** is essential, with the Reserve Bank of India (RBI) leading the charge to establish a unified fraud intelligence platform for real-time data sharing among financial institutions. Finally, and most critically, a sustained **nationwide consumer education campaign** is needed to empower the public with the knowledge to recognize and resist social engineering scams. By combining robust technology, regulatory oversight, and an informed public, India can build a more secure and resilient digital banking ecosystem, safeguarding its economic future and the confidence of its citizens.

12.BIBLIOGRAPHY

BOOKS

- Gupta, S. (2023). Electronic Banking Frauds: The Case of India. In *Electronic Banking Frauds: The Case of India* (pp. 166-180). IGI Global.

ISSN: 2582-6433

JOURNALS

- Maini, R., & Sindhi, V. K. (2025). Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance. *International Journal of Finance and Management Research, 7*(5). DOI: 10.36948/ijfmr.2025.v07i05.55593.
- Ramya, Mrs. & Raj G, Suresh Mathew. (2024). Laws Regulating Online Banking Frauds in India: A Comparative Study with Existing Laws in USA. *AARJ, XIV*, 3-4.
- Sharma, Dr. Uma Shanker. (2015). A Study on Legal Framework in Indian E-Banking System. *AIJRA, III*(I).
- Singh, Charan. (2024). Frauds in the Indian Banking Industry: An Analysis. *IIMB Working Paper No. 505*. Retrieved from https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf.

ARTICLES AND REPORTS

- A. B. Karki, *Strategic Approaches for Combating Digital Financial Fraud in 2025* (Feb. 14, 2024), https://bankiq.co/effective-strategies-to-mitigate-digital-financial-frauds-in-2025 (last visited Sept. 15, 2025).
- A. K. Jain, *Cyber Security Tips*, Union Bank of India, https://www.unionbankofindia.co.in/en/common/cyber-security (last visited Sept. 15, 2025).
- A. K. Jha, *Airtel Payments Bank Launches 'Safe Second Account' to Boost Secure Digital Transactions* (Sept. 22, 2025), **Times of India**, https://timesofindia.indiatimes.com/technology/tech-news/airtel-payments-bank-launches-safe-second-account-to-boost-secure-digital-transactions/articleshow/124053118.cms (last visited Sept. 15, 2025).
- V. S. Kaveri, *Powerful Strategies to Combat Banking Frauds in India*, Indiaforensic, https://indiaforensic.com/powerful-strategies-to-combat-banking-frauds-in-india (last visited Sept. 15, 2025).
- S. G. Pande, *Powerful Strategies to Combat Banking Frauds in India*, Indiaforensic, https://indiaforensic.com/powerful-strategies-to-combat-banking-frauds-in-india (last visited Sept. 15, 2025).
- PTI, *RBI Issues Revised Guidelines for Payment Aggregators to Enhance Consumer Protection* (Sept. 17, 2025), **News on Air**, https://www.newsonair.gov.in/rbi-issues-revised-guidelines-for-payment-aggregators-to-enhance-consumer-protection (last visited Sept. 15, 2025).

ISSN: 2582-6433

- Rahi Bhattacharjee, *RBI Annual Report FY24: What Caught Our Attention?* (June 1, 2025), **Bureau**, https://bureau.id/resources/blog/rbi-annual-report-fy24-what-caught-our-attention (last visited Sept. 15, 2025).
- M. S. Singh & P. K. Saxena, *How Technology Can Redefine Fraud Detection in Indian Banking Sector* (Dec. 23, 2024), **ET Edge Insights**, https://etedge-insights.com/technology/cyber-security/how-technology-can-redefine-fraud-detection-in-indian-banking-sector (last visited Sept. 15, 2025).
- *Banking Fraud and Its Preventive and Detective Mechanism in Indian Perspective*, **ResearchGate**, https://www.researchgate.net/publication/357822213_Banking_Fraud_and_its_Preventive_and_Detective_Mechanism_in_Indian_Perspective (last visited Sept. 15, 2025).
- **Reserve Bank of India**, *Report on Trends and Progress of Banking in India* 85 (2023), https://www.rbi.org.in (last visited Sept. 15, 2025).
- **Reserve Bank of India**, *Cyber Security Framework in Banks* (2016), https://www.rbi.org.in (last visited Sept. 15, 2025).
- **Reserve Bank of India**, *Annual Report 2023–24* (2024), https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1214 (last visited Sept. 15, 2025).
- **Press Information Bureau**, Ministry of Electronics & Information Technology, *Phishing Attacks on Digital Payment Users Rise in India* (Mar. 14, 2023), https://pib.gov.in (last visited Sept. 15, 2025).
- **KPMG**, *Fraud Survey: Navigating the New Age of Cybercrime in Indian Banking* 34 (2022), https://kpmg.com (last visited Sept. 15, 2025.