The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 4 | April 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Challenges and Legal Issues in Mobile Banking in India

Aakriti Chauhan

ARTICLE DETAILS

Research Paper

Accepted: 17-04-2025

Published: 10-05-2025

Keywords:

Cybersecurity, Data Privacy, Identity Theft, Mobile banking, R.B.I

ABSTRACT

This research article delves into the multifaceted challenges and legal issues surrounding mobile banking in India. As mobile banking becomes increasingly integral to the nation's financial ecosystem, concerns related to cybersecurity, data privacy, digital illiteracy, and regulatory compliance have emerged prominently. The study explores the current legal framework governing mobile banking, including the role of the Reserve Bank of India and relevant statutes, while highlighting gaps in enforcement and awareness. It also examines the vulnerabilities users face, such as phishing, identity theft, and unauthorized transactions, emphasizing the need for more robust technological safeguards and consumer protection mechanisms.The study concludes that while mobile banking fosters financial inclusion and convenience, it necessitates an evolving and resilient legal regime to address emerging risks and ensure secure digital financial transactions.

DOI : https://doi.org/10.5281/zenodo.15390374

INTRODUCTION

Mobile banking denotes the use of mobile devices for banking transactions such as money transfer, bill payment, balance enquiry and loan application[1]. It serves as a fast, secure and more convenient option as compared to traditional banking as there is less need to carry physical bank documents and ATM cards to perform basic banking functions[2]. Mobile banking serves a very important function in the development of financial inclusion in India, where limited access to banking infrastructure remains a concern[3].

Growth and adoption friends in India:

India has recent growth rate in mobile banking for several reasons:

1) increase in smartphone access: over 750 million smartphone users in India contributing to mobile banking adoption.

2) increase in upi transaction volume: upi transactions reached over 10 billion transactions monthly in 2023.

3) the growth of intact markets: usage of mobile apps such as Gpay ,phonepe, Paytm, and Bhim has changed phone experience for mobile banking significantly.

Government initiatives:

Different government supported programmes such as digital India Jan dhan Yojana Aadhar link bank has helped to support mobile banking and also addressed the wider customer base.[1]

Need for Legal Regulation in Mobile Banking

The exponential growth of mobile banking in India has been both a boon and a challenge. With the increasing smartphone penetration and the government's push for a cashless economy through initiatives like Digital India, mobile banking has become a critical tool for financial inclusion. However, this convenience has been accompanied by a surge in legal and regulatory concerns, making effective legal regulation indispensable. Mobile banking transactions involve sensitive financial and personal data, exposing users to risks like cyber fraud, data breaches, unauthorized transactions, and identity theft[5]. To address these risks, legal regulation is essential to protect consumers from exploitation and ensure financial accountability.

One of the most pressing issues is the protection of consumer rights, especially for those with low digital literacy, who often fall victim to scams and phishing attacks. The Reserve Bank of India (RBI) has launched several initiatives such as the Integrated Ombudsman Scheme, 2021, to streamline grievance redressal mechanisms and hold financial institutions accountable.[6] Additionally, data privacy and

[1] Reserve Bank of India, Report on Trends and Progress of Banking in India 2022-23, RBI Publications.
[2]KPMG Report on "Digital Banking in India: 2023 Outlook."
[3]World Bank, "Financial Inclusion and Mobile Banking in Developing Countries," 2022.
[4]Telecom Regulatory Authority of India (TRAI), "Annual Telecom Data Report 2023."

cybersecurity are at the forefront of mobile banking regulation, as banks and fintech apps collect vast amounts of personal data. The Digital Personal Data Protection Act, 2023. marks a significant step forward, requiring entities to process data lawfully, ensure consent-based access, and impose penalties for misuse or breach.[7]

The threat of cybercrime has also amplified, as cybercriminals target mobile platforms with tactics such as SIM swapping, malware, and OTP fraud. The Information Technology Act, 2000, under Sections 43 and 66, provides the foundational legal framework for punishing data theft and cyber offences. Moreover, regulatory oversight of fintech companies has become crucial, given that many non-banking financial entities now offer mobile-based services without being under the same scrutiny as licensed banks.[2]

CHALLENGES IN MOBILE BANKING IN INDIA

1*) Cybersecurity threats*: cyber crime has increased substantially with more incidents of phishing attacks, sim card fraud ,malware and hacking, despite the need for two factor authentication for fraudsters who have found ways around security. The RBI noticed an increase of 46% in mobile banking fraud cases in the past 5 years[8].

2*) data privacy and protection challenges*: Mobile banking apps gather massive amounts of personal and financial data about the user which leaves the user exposed to identity theft and financial issues. India does not have extensive laws governing data protection laws.one of the bills that is the personal data protection bill 2019 still under consideration [34]that aims to regulate data security. According to IT act 2000 banks must adopt adequate security measures however implementation lacks uniformity[9].

[2][5]Bhandari, V. (2023). Mobile Banking and Legal Risks in India, Journal of Financial Regulation and Compliance, Vol. 31, Issue 2, pp. 104–116.
[6]Reserve Bank of India, Integrated Ombudsman Scheme, 2021, [Press Release], November 12, 2021. Available at: www.rbi.org.in.
[7]Ministry of Electronics and Information Technology (MeitY), The Digital Personal Data Protection Act, 2023, Gazette Notification, August 2023.
[3][8]State of Maharashtra v. Dr. Praful B. Desai, AIR 2003 SC 2053 – The Supreme Court recognized the admissibility of electronic evidence, relevant in prosecuting cyber crimes in mobile banking fraud cases.
[9]K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 – The Supreme Court declared the right to privacy as a fundamental right under Article 21, establishing a constitutional foundation for data protection in mobile banking.

3). Consumer awareness and digital literacy: Significant number of users predominantly from ruler and semi urban reasons do not comprehend the importance of digital security therefore making them easy targets for scam customer are being misled to the use of phishing, fake banking applications and even social engineering .while RBI and other banks run awareness campaigns regarding cyber security the level of digital literacy continues to be very poor[10].

4*). Regulatory concerns* : Both bank and Fintech companies struggle to meet rapidly changing know your customer(kyc) requirements, anti money laundering policies and RBI digital banking regulations. Moreover, fintech companies dealing with digital lending and payment services tend to bypass conventional banking laws resulting in regulatory gaps[11].

5). Fraudulent transactions and liability of consumer :The rise of unauthorised digital transactions has led to disputes regarding the liability of consumers. While the RBI has established a franchisee policy to protect consumers from losses in such transactions, many victims experience difficulties in demonstrating the fraud which therefore extends the time before they are refunded for their loss.

The lack of centralized detection of fraud and monitoring also adds to the challenge of protecting consumers[12].[5]

LEGAL ISSUES IN MOBILE BANKING

1).Gaps in Data Protection Laws

India is still working on a solid data protection law. The proposed Digital Personal Data Protection Bill is meant to set rules for how financial data is collected and used, but it hasn't been put into action yet.[13]

2).Jurisdictional Challenges in Digital Transactions

[10]Shreya Singhal v. Union of India, AIR 2015 SC 1523 – The court emphasized the need for clarity in digital communication regulations and struck down vague cyber provisions that could impact digital awareness campaigns.
4

5 [11]Reserve Bank of India v. Jayantilal N. Mistry (2016) 3 SCC 525 – This case addressed regulatory authority and confidentiality in financial institutions, highlighting issues around oversight in fintech operations.
[12]RBI Circular on "Limiting Liability of Customers in Unauthorized Electronic Banking Transactions", July 6, 2017 – Provides the legal foundation for customer protection and liability in digital fraud cases.

When it comes to online banking fraud, things can get tricky because these cases often cross borders. Courts find it tough to figure out which jurisdiction applies, especially when foreign entities are involved.[14]

3).Compliance Burden on Banks and Fintechs

The Reserve Bank of India (RBI) has strict KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations in place, but how well these rules are enforced can vary quite a bit.

4).Unauthorized Lending Apps

There are illegal digital lending apps out there that take advantage of users by charging sky-high interest rates and using harsh recovery methods. In December 2024, the Indian government proposed a law to criminalize unregulated lending, with penalties that could include up to seven years in prison.

5*).Lack of Comprehensive Data Protection Law*

Absence of a robust personal data protection regime increases the risk of data misuse and privacy breaches.

6).Jurisdictional Challenges in Dispute Resolution

Transactions occurring across states or countries create complications in determining legal jurisdiction.

RECENT JUDICIAL DEVELOPMENTS, LEGAL FRAMEWORK AND CASE LAWS

Recent Developments in Digital Banking

Bank Accountability for Unauthorized Transactions

In a groundbreaking decision, the Kerala High Court ruled that banks can't just wash their hands of responsibility for unauthorized withdrawals, even if customers don’t reply to SMS alerts.[15] The court made it clear that banks have a responsibility to take reasonable steps to safeguard their customers' interests and must set up systems to block unauthorized transactions. This ruling highlights the judiciary's commitment to putting consumer protection front and center in the world of digital banking.

Concerns About the Surge in Online Banking Frauds:

The Delhi High Court has raised alarms about the rising tide of online banking frauds. They pointed out that while online banking has become a part of our everyday lives, it has also opened the door for scammers who take advantage of people's trust. This highlights the increasing awareness within the judiciary regarding cybersecurity risks in the world of digital banking and emphasizes the urgent need for stronger protective measures.

Legal Framework of Mobile Banking

The legal framework governing mobile banking in India is a composite of various laws, regulations, and guidelines issued by statutory bodies like the Reserve Bank of India (RBI), Information Technology Act, and other sectoral regulators. Below is a detailed overview of the legal framework:

The legal framework governing mobile banking in India is a composite of various laws, regulations, and guidelines issued by statutory bodies like the Reserve Bank of India (RBI), Information Technology Act, and other sectoral regulators. Below is a detailed overview of the legal framework:

1).Reserve Bank of India (RBI) Guidelines

The RBI is the chief regulator for mobile banking in India. Key regulations include:

a. Mobile Banking Regulations (2008 & onwards)

- RBI issued guidelines in October 2008 allowing banks to offer mobile banking services with prior approval.[16]

- Mandates two-factor authentication for all financial transactions.

- Emphasizes security standards, transaction limits, and grievance redress mechanisms.

b. KYC/AML Guidelines

- Banks must comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) norms under the Master Directions on KYC, 2016.

c. Prepaid Payment Instruments (PPIs) Guidelines

- Issued under the Master Direction on PPIs.These regulate mobile wallets and UPI apps.

- Lay down eligibility criteria, loading limits, and permissible credits/debits.

[6]d. Unified Payments Interface (UPI) Guidelines

- Governed by NPCI (National Payments Corporation of India), regulated by RBI.

- Include norms on security, interoperability, and third-party application providers (TPAPs).

2. Information Technology Act, 2000 (IT Act)

The I.T Act Provides the legal recognition of electronic transactions and digital signatures.

Key Provisions:

- Section 43 & 66: Penalize unauthorized access and cyber frauds.

- Section 72: Protects privacy and confidentiality of user data.

- Section 79:Safe harbor for intermediaries like payment gateways, subject to due diligence.[17]

3. Payment and Settlement Systems Act, 2007

- Empowers RBI to regulate all forms of payment systems, including mobile banking.[18]

- Ensures the security and efficiency of payment channels like NEFT, RTGS, IMPS, and UPI.

4.Consumer Protection Act, 2019

- Protects consumers from unfair trade practices and deficient services, including those related to mobile banking.

- Consumers can seek redressal in consumer forums for unauthorized transactions or service failures.

5. Data Protection Framework (Pending Legislation)

- The Digital Personal Data Protection Act, 2023 is set to play a crucial role in protecting user data in mobile banking.

- Emphasizes user consent, data minimization, and grievance mechanisms for personal data misuse.

---

[6] [16]Reserve Bank of India, Mobile Banking Transactions in India – Operative Guidelines for Banks Circular No. RBI/2008-09/215, October 8, 2008

6. Indian Penal Code (IPC) & Bharatiya Nyaya Sanhita (BNS)

- Provisions under IPC/BNS can be invoked for fraud, identity theft, and cybercrime related to mobile banking.

Case Laws:

1).ICICI Bank Limited v. Uma Shankar Sivasubramanian

In this case, the Kerala High Court addressed a SIM swapping fraud where fraudsters gained access to the petitioner's bank account and withdrew funds. The court emphasized the bank's duty to protect its customers' interests and held that banks cannot absolve themselves of liability for unauthorized transactions, even if customers fail to respond to SMS alerts. This judgment underscores the judiciary's stance on prioritizing consumer protection in the digital banking landscape.[17]

2).State Bank of India v. Pallabh Bhowmick & Ors

The Supreme Court ruled that the State Bank of India (SBI) is liable for fraudulent and unauthorized transactions that occurred on a customer's account. This particular case revolved around a customer who was a victim of cyber fraud, leading to a loss of ₹94,204.80. Even though the bank tried to argue that the customer was negligent, the Court found SBI accountable. They referenced the Reserve Bank of India (RBI) Circular from July 6, 2017, which guarantees "zero liability" for customers who quickly report unauthorized transactions that arise from third-party breaches.[18]

3).Vodafone Cellular Limited v. Sanjay Govind Dhande and Others

In this case there was a troubling incident of sim card fraud, an imposter managed to get their hands on a duplicate SIM card that was tied to the complainant's mobile number, which then allowed them to carry out unauthorized transactions from the complainant's bank account. The court took a close look at how the telecom company issued this duplicate SIM without doing the necessary checks, leading to those unauthorized bank transactions. This case really shines a light on the urgent need for telecom operators and banks to implement stricter verification processes to help prevent these kinds of frauds in the future.[19]

RECOMMENDATIONS AND FUTURE OUTLOOK

The swift growth of mobile banking in India brings a mix of exciting opportunities and significant challenges. On one hand, we're seeing more people gain access to financial services, but on the other, there are still important legal and security concerns that need to be addressed. Here are some recommendations to consider:The recommendations and future outlook presented here are designed to strengthen regulatory frameworks, improve cybersecurity measures, and boost consumer protections within India's mobile banking sector.

RECOMMENDATIONS

1).Strengthening Regulatory Frameworks:

The Reserve Bank of India (RBI) should formulate stricter compliance requirements for mobile banking service providers requiring more frequent cybersecurity audits.

2). Boosting Cybersecurity measures:

Banks need to make sure customers use more than one way to prove who they are. This means going beyond one-time passwords. They should think about using things like fingerprints or special security devices

3).Consumer Awareness and Protection:

The Reserve Bank of India (RBI) and financial institutions ought to implement comprehensive financial literacy initiatives across the country to inform consumers about phishing scams, deceptive applications, and secure digital banking methods.

4).Collaboration Between Telecom and Banking Sectors:

Telecom providers must be required to enforce more rigorous KYC (Know Your Customer) verification processes prior to the issuance of duplicate SIM cards, in order to combat SIM swap fraud effectively.

FUTURE OUTLOOK

1).Evolution of Legal Frameworks:

India is expected to establish a dedicated regulatory authority for fintech to oversee mobile banking and digital payment systems.

2).Incorporating AI with Blockchain:

Artificial intelligence (AI) and blockchain technology will be instrumental in improving security, identifying fraudulent activities, and streamlining regulatory compliance processes.

3).Emergence of Central Bank Digital Currency:

The launch of the Digital Rupee (CBDC) by the Reserve Bank of India (RBI) is set to transform mobile banking by offering a secure digital payment option supported by the government, significantly reducing the potential for fraud.

4).Global Regulatory Alignment:

India aims to synchronize its digital banking regulations with international standards by working alongside global financial regulators to address issues related to cross-border cyber fraud and money laundering.

CONCLUSION

Mobile banking in India has transformed the financial sector by promoting financial inclusion, enhancing convenience, and driving economic growth. However, this rapid development has also brought forth various challenges, such as cybersecurity risks, concerns over data privacy, regulatory deficiencies, and ambiguities regarding consumer liability in fraud cases. The legal framework that governs mobile banking, which includes RBI regulations, the IT Act, and the forthcoming Digital Personal Data Protection Bill, is essential for addressing these challenges.

Recent judicial decisions have strengthened consumer protection by making banks and telecom providers liable for unauthorized transactions and fraudulent activities. Despite these advancements, there is an urgent need for enhanced cybersecurity protocols, more robust regulatory oversight, and greater consumer education to reduce potential risks.

REFERENCES

BOOKS

- Singh, Yatindra. Cyber Laws. Universal Law Publishing, 2022.

- Sharma, Vakul. Information Technology: Law and Practice. Universal Law Publishing, 2023.
- Rao, M. B. & Rao, Manjula Guru. Cyber Crimes and Legal Measures. Eastern Book Company, 2021.
- Chand, Vikram. Banking Laws and Practices in India. LexisNexis, 2023.

JOURNAL ARTICLES

- Bansal, Sakshi. "Mobile Banking in India: Issues, Challenges and Prospects." International Journal of Research in Economics and Social Sciences, Vol. 10, Issue 6, 2020.
- Tiwari, Rajeev & Buse, Stephan. "The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector." Journal of Internet Banking and Commerce, Vol. 15, No. 1, 2021.
- Kumari, Ritu. "Cyber Security and Digital Banking in India." International Journal of Law Management & Humanities, Vol. 5, Issue 3, 2022.
- Kapur, Vikas. "Legal and Regulatory Framework for Mobile Banking in India." Indian Journal of Law and Technology, Vol. 18, Issue 1, 2022.

Newspaper Articles

- The Hindu, "Kerala HC Holds Banks Liable for Unauthorized Transactions," Dec. 20, 2023.
- The Indian Express, "Digital Banking Fraud on the Rise: What You Need to Know," Jan. 5, 2024.
- Economic Times, "RBI Flags Surge in Mobile Banking Frauds," Oct. 15, 2023.
- Hindustan Times, "New Data Protection Law to Reshape Digital Banking," Aug. 20, 2023.

REPORTS

- Reserve Bank of India, Annual Report 2022–23, available at: https://rbi.org.in
- Ministry of Electronics and IT (MeitY), Digital India Programme Overview, https://digitalindia.gov.in
- National Payments Corporation of India (NPCI), UPI Transaction Data, https://www.npci.org.in