VOLUME - 15, ISSUE - 08, AUGUST - 2026 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Law

SAFEGUARDING WOMEN IN THE DIGITAL BANKING ECOSYSTEM: A SYSTEMATIC REVIEW OF INDIAN CYBER JURISPRUDENCE AND REGULATORY FRAMEWORKS

Chavhan Pradip Mohan

Research Scholar, Department of Law, Monark University, Vahelal, Ahmedabad, Gujarat, India.

ABSTRACT

Various demographic groups in India now have easier access to banking services because to the fast digitisation of the industry, which has been fuelled by innovations like the Unified Payments Interface (UPI), online banking, and fintech platforms. On the other hand, cyber-enabled financial crimes targeting women have increased in number with this architectural growth. bank crimes targeting women include deceitful schemes, "digital arrests," extortion via compromised bank credentials, identity theft, and unauthorised electronic currency transfers. The purpose of this study is to provide a comprehensive examination of the laws, case law, administrative rules, and frameworks that regulate the safety of women's digital banking in India. This paper evaluates the institutional barriers, legal recourse, and liability allocation regimes that women face in India by analysing important statutory instruments such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), and the Digital Personal Data Protection Act, 2023 (DPDPA).

KEYWORDS : Cybercrime, Women safety, Banking, BNS, Digital transactions etc.

INTRODUCTION

A huge policy change has occurred in India with the move toward a cashless economy. As a result of the "India Stack"—a network of public digital infrastructure—millions of women in India have gained access to formal banking services via online payment systems. Systemic gender vulnerabilities continue to limit digital financial inclusion, notwithstanding recent achievements. Due to factors such as lower levels of digital literacy, social engineering, targeted cyber-harassment associated with financial extortion, and structural barriers in navigating regulatory grievance redressal systems, female users of the digital financial ecosystem face asymmetric risk profiles. In the realm of finance, cybercrime targeting women has progressed beyond simple card-cloning operations. It has progressed into intricate, multi-tiered scams, encompassing:

1. Phoney frauds (such as pretending to be a law enforcement official and making "digital arrests");
2. SIM switching without authorisation;
3. Harassment via loan apps including non-consensual picture alteration and unauthorised acquisition of personal contact lists;
4. Phishing and vishing thru synthetic deep fakes.

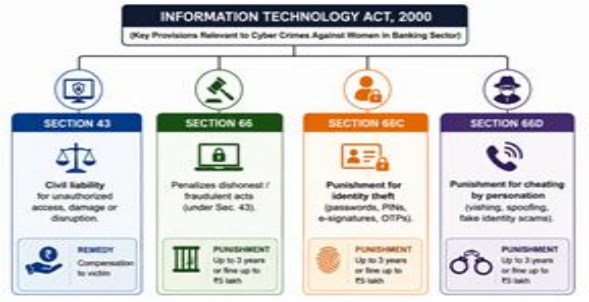
This study offers a comprehensive analysis of the gender-sensitive frameworks and cyber jurisprudence in India's banking sector. It lays out the essential changes to prevent financial cybercrimes against women and assesses whether the existing legal safeguards, penalties, banking compliance standards, and court orders do enough to protect them.

Methodology

A doctrinal and normative research technique is used in this comprehensive literature and legal examination. The legal precedents from the Indian Supreme Court and other High Courts, as well as regulatory circulars, statutory regulations, and clauses are all examined by the framework. The principal cyber legislation in India is the Information Technology Act, 2000 (IT Act). (IT Act). Measures aimed squarely at protecting female bank clients from cyber fraud and identity theft include as follows:

Section 43 (Penalty and Compensation for Damage to Computer System): Makes people legally liable when they break into computer systems, steal data, or cause disruptions. Malware or unauthorised remote access programs may compromise victims' devices, and this law requires compensation remedies for them.

Section 66 (Computer Related Offences): It makes dishonest or fraudulent activities listed in Section 43 a crime punishable by penalties up to five lakh rupees or jail terms of up to three years.



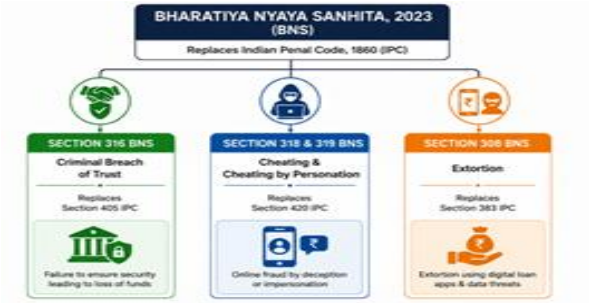
Section 66C (Punishment for Identity Theft): Theft of digital signatures, passwords, or other forms of unique identification (such bank PINs or one-time passwords) is the direct subject of this attack. Under the guise of upgrading KYC credentials, fraudsters often target women by stealing one-time passwords (OTPs).

Section 66D (Punishment for Cheating by Personation by Using Computer Resource): Discusses methods used in vishing, spoofing, and false identity schemes in which con artists impersonate legitimate entities such as banks, governments, or police forces. Unlike overbroad laws, Section 66D explicitly addresses fraudulent impersonation including clear mens rea, as shown in the Supreme Court's upholding of Section 66D's constitutional validity and need in Shreya Singhal v. Union of India (2015).

Bharatiya Nyaya Sanhita, 2023 (BNS)

The Bharatiya Nyaya Sanhita, 2023 (BNS) revised criminal terminology to deal with crimes that are made possible by cyberspace after the Indian Penal Code, 1860 (IPC) was repealed:

Section 316 BNS (Criminal Breach of Trust): In cases when intermediaries or financial institutions entrusted with client assets do not implement necessary security procedures, resulting in the illicit syphoning of capital, this section supersedes Section 405 of the Indian Penal Code.



Section 308 BNS (Extortion): Updates and supersedes Section 383 of the Indian Penal Code. This clause is crucial in combating illicit digital lending applications that prey on women by stealing their personal information, photos, and financial data and then threatening them with public shame until they pay exorbitant interest.

Digital Personal Data Protection Act, 2023 (DPDPA)

Digital Personal Data Protection Act, 2023's passage signalled a sea change in data reduction and transparency regulations: **Section 6 (Obligations of Data Fiduciary):** Financial technology platforms and banks are considered data fiduciaries according to Section 2(i). Strictly for authorised and permissible reasons, they are obligated to handle personal financial data.

Section 8 (Organizational Safeguards and Data Breach Notification): Requires Data Fiduciaries to take reasonable precautions to avoid unauthorised access to personal information. In order to mitigate the possibility of concealed vulnerabilities, banks are required under Section 8(6) to inform the Data Protection Board of India and impacted persons in the case of a personal data breach impacting female customers.

Reserve Bank of India (RBI) Regulatory Frameworks and Liability Regimes

The regulatory framework established by the Reserve Bank of India (RBI) serves as the operational frontline in addressing victim redress, account security, and responsibility allocation in unauthorised digital transactions, while statute enactments provide criminal and civil consequences. When it comes to banking, non-bank financial companies (NBFCs), and non-bank systemic payment system operators (NSPOs), the Integrated Ombudsman Scheme brings it all together. It sets up a simple way for women to dispute chargebacks, unaccredited unauthorised debit entries, and unresolved banking complaints.

Judicial Precedents and Evolving Cyber Jurisprudence

In order to safeguard vulnerable banking customers, respond to new forms of cybercrime, and strengthen data privacy, Indian courts have interpreted cyber and financial laws.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1

According to a nine-judge panel of India's highest court, Article 21 guarantees citizens the right to privacy, which is an essential component of the right to life and personal liberty. The Court stressed that privacy includes rights to one's own body, to one's own decisions, and to one's own personal information. This precedent, when applied to online banking, requires all financial institutions to provide stringent technological protections for customers' private financial information.

Shreya Singhal v. Union of India (2015)

The IT Act's Section 66A was struck down by the Supreme Court for being too broad, while Section 66D was explicitly maintained. The Court noted that Section 66D deals with separate crimes involving computer-based impersonation and cheating, creating a legitimized tool to combat impersonation schemes, which prey on female bank customers more than males.

CBI v. Arif Azim (2003) [Sony Sambandh Case]

This case, which was one of the first of its kind in India, proved that the IT Act and punitive statutory provisions pertaining to impersonation and cheating make it illegal to commit crimes like identity theft and unauthorised use of credit on online platforms.

Institutional Mechanisms and Regulatory Gaps

1. The Mule Account Infrastructure

The "mule account" is the main channel by which cyber financial fraud is perpetrated. This kind of bank account is created using hacked or fake KYC credentials, and its purpose is to quickly receive and withdraw stolen cash. Even tho the Reserve Bank of India (RBI) has issued directions requiring real-time transaction monitoring and stringent Know Your Customer (KYC) compliance, fraudsters still manage to bypass freeze requests by taking advantage of digital onboarding pipelines' inadequate monitoring systems.

2. Friction in Real-Time Money Freezing

One resource that may be used to track and freeze fraudulent transactions in real-time is the National Cyber Crime Reporting Portal (NCRP) and its emergency helpline (1930). But thieves may often get their hands on cash via ATMs or turn it into crypto currency before account freezes are put into effect because of institutional delays in communication between police departments and bank fraud-control divisions.

3. Restrictive Interpretation of "Customer Negligence"

Financial institutions sometimes try to avoid bearing the responsibility of showing client carelessness by claiming that an OTP or static password was input during the transaction, even tho RBI directives say that the bank is the one that must prove customer negligence.

Recommendations and Regulatory Reforms

A combination of legislative, regulatory, and technical changes is necessary to shore up these weak spots and make online banking a safer environment for women.

1. Legislative Amendments and Statutory Definitions

Statutory Recognition of Coerced Consent: To make it clear that authorisation gained via deceit, psychological pressure ("digital arrest"), or coercion does not constitute valid authorisation or consumer carelessness, amend the financial fraud definitions under the IT Act and BNS.

Enhanced Penalties for Extortion Loan Apps: To penalise organisations that gather personal data for financial debt collection without express and verifiable authorisation, the IT Act should include strong liability measures.

2. Regulatory Directives by the Reserve Bank of India

Mandatory Cooling-Off Periods for High-Value Transactions: Initiate first-time electronic financial transfers above set levels from new devices or unexpected geographical areas and mandate a dynamic, risk-based cooling-off phase.

AI-Driven Transaction Anomaly Detection: Banks must implement AI systems that can detect suspicious patterns of transfers, alert authorities to possible mule accounts, and temporarily hold debits with a high risk of fraud until final settlement.

Liberalized Ombudsman Standards: In cases when social engineering or psychological coercion is shown, the simple submission of an OTP does not always constitute proof of client fault. This clarification should be sent to the Banking Ombudsman.

3. Institutional and Capacity-Building Reforms

Specialized Cyber Grievance Desks for Women: To enable victims of financial cybercrimes report they quickly and empathically, set up cyber helpdesks manned by women at local police stations and online.

Targeted Digital Financial Literacy Initiatives: Collaborate with Panchayats and Urban Local Bodies to educate female customers on digital security, authentication methods, and quick post-fraud reporting procedures via specialised

financial literacy initiatives launched under Helpline 1930.

CONCLUSION

There is a great deal of untapped potential in India's digital financial ecosystem to increase financial inclusion and empower women customers. The expansion, however, is still open to cyber-enabled financial crimes that prey on gender, structural, and technological weaknesses. Strong regulatory enforcement and victim-centric judicial interpretation are crucial for the success of the statutory architecture that includes the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023.

Article 21 of the Indian Constitution mandates the protection of personal information and financial assets against digital theft, as confirmed by the country's highest court in the Puttaswamy case and subsequent directions on cybercrime. India can create a digital banking environment that is safe for women and the law by removing mule account networks, implementing proactive banking compliance measures, addressing regulatory gaps, and creating methods to address grievances based on gender.

REFERENCES

1. Reserve Bank of India Master Circular on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions, DBR.No.Leg.BC.78/09.07.005/2017-18.
2. Tripathy, S. S. (2025). Psychological strategies, social engineering, and vishing mechanisms in digital financial crimes. Legal Review Quarterly, 12(2), 78–95.
3. Sharma, R., & Gupta, P. (2022). Legal challenges in banking-related cyber fraud and consumer liability. Indian Journal of Law and Technology, 18(1), 23–45.
4. Bhadoriya, T. (2023). Cyber crime against women: Challenges and prevention in the digital landscape. International Journal of Law and Legal Jurisprudence Studies, 10(3), 114–132.