ORIGINAL RESEARCH PAPER

Law

KEY WORDS: Digital Banking Security, Women Cyber Safety, Financial Fraud in Banking, IT Act 2000, Bharatiya Nyaya Sanhita 2023, UPI Security etc.

CYBERCRIMES AGAINST WOMEN IN DIGITAL BANKING: LEGAL CHALLENGES AND REGULATORY RESPONSES IN INDIA

Chavhan Pradip Mohan

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

ABSTRACT

Mobile banking apps, the Unified Payments Interface (UPI), and Aadhaar-enabled payment mechanisms have sped up the digitisation of banking in India, making it possible for millions more people to have access to official financial services. Unfortunately, with the fast spread of digital services has come an increase in online financial exploitation and digital banking fraud, which disproportionately affects women who use these services. While technology perimeters have been strengthened in contemporary banking architecture to prevent direct database breaches, hackers are becoming more adept at exploiting human weaknesses via social engineering, identity theft, misleading UPI collect requests, vishing, and coercive intimidation. This essay delves deeply into the socio-legal aspects of cybercrimes committed against women in India's online banking industry. It examines the current legislative framework, including the Information Technology Act, 2000, and recent penal reforms under the Bharatiya Nyaya Sanhita, 2023, as well as empirical trends from official cybercrime repositories and reasons that increase the vulnerability of women, such as culture, behaviour, and structure. In addition, the research delves into the systematic procedural obstacles that hinder investigation, evidence gathering, and victim compensation as per the rules set by the Reserve Bank of India.

INTRODUCTION

A hyper-connected, real-time digital infrastructure has replaced the old, brick-and-mortar branch operations in India's financial services ecosystem, which has changed drastically over the last 20 years. Thanks to forward-thinking public policy initiatives, the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI), instant payment networks like the Unified Payments Interface (UPI), mobile banking apps, and biometric authentication platforms have completely transformed the way people manage their personal finances. The entry of millions of previously unbanked individuals, informal workers, and rural families into the formal sector has been facilitated by this digital migration, which has also acted as a major accelerator for financial inclusion. Especially for women, digital banking has brought a new level of independence, letting them handle their own funds, get direct benefit transfers (DBT), shop online, and get micro-credit all without having to deal with male middlemen or physically visit bank offices.

The fast shift to digital has, however, coincided with an increase in digital threat vectors. Cybercriminals have moved their focus from technological exploitation to psychological manipulation as cryptographic protocols, multi-factor authentication, and end-to-end encryption have strengthened the key software perimeters of financial technology businesses and commercial banks. Social engineering, which involves influencing people's actions, beliefs, and prejudices in order to circumvent technological safeguards, is now the primary tactic used in online banking fraud. Because of this change in security norms, female bank account holders are now considered easy prey for criminals. As a result of unique weaknesses that fraudsters routinely take advantage of, the confluence of fast digital adoption and pervasive socio-cultural disparities has emerged.

Disparities in socioeconomic status, digital operational literacy, and access to devices contribute to the sexism in cyber banking fraud in India. Even if more and more Indian women are using the internet, there is still a long way to go before they can confidently handle modern cybersecurity threats. Many women in semi-urban and rural families use shared family mobile devices, have less technical knowledge about multi-factor authentication techniques, or need someone else to help them when they bank online.

Intersectional Vulnerabilities and Modus Operandi in Digital Financial Fraud

A thorough examination of the socio-behavioral dynamics and particular fraud typologies used by those responsible for perpetrating digital banking crimes against women is necessary in order to comprehend their mechanics. Criminals that operate online seldom use cookie-cutter approaches, preferring instead to target certain demographics and socioeconomic groups. Social and cultural status, traditional gender roles at home, and career goals are key considerations for female customers when developing these tactics. There are four main operating models that women face when it comes to digital banking fraud:

Deceptive UPI Collect Requests and QR Code Exploitation

Although UPI has become the preferred payment method in India due to its widespread use and ease of use, scammers sometimes exploit its vulnerabilities. Con artists often target women who are involved in secondary markets, micro-enterprises, or peer-to-peer transactions conducted online. Con artists pose as customers or clients in an effort to trick them into parting with their money. A thief may use a misleading QR code or a "UPI Collect" request to trick victims into sending upfront payment. Accidentally authorising a debit from her bank account, the victim acts under the false impression that receiving money requires scanning a code or entering her Unified Payments Interface PIN.

Banking Vishing and KYC Impersonation

Phishers using voice phishing, often known as "vishing," pose as legitimate banking personnel, customer service representatives, or payment gateway verification agents. These con artists approach female account holders using phone impersonation services and threaten to suspend their main bank account, debit card, or digital wallet if they do not comply with Know Your Customer (KYC) regulations. The criminal takes advantage of the victim's fear and the victim's lack of confidence in the institution to get sensitive authentication credentials that are then utilised to conduct illegal electronic transfers..

Fraudulent Part-Time Job and High-Yield Investment Schemes

Thru social media and instant messaging platforms, cyber syndicates disseminate misleading advertising aimed at housewives, recent college grads, and women looking for remote employment possibilities. For doing something as easy as like a video stream, rating an ad listing, or writing a review of a digital product, many programs provide daily earnings that may be rather valuable. In order to establish confidence, victims are first given small reimbursements into their bank accounts. Under the guise of unlocking higher profit tiers, the operators then force the victim to transfer large quantities of money into fake "prepaid task accounts" or unregistered investment websites. The con artists steal the victim's hard-earned money by freezing the gateway the moment she tries to withdraw it, then demanding further imaginary fees.

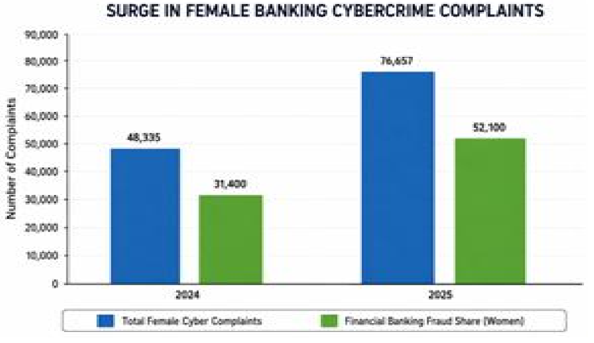
Coercive Intimidation and Synthetic Legal Threats

"Digital arrest" and legal impersonation frauds, which use psychological coercion, are a particularly harmful kind of cyber fraud. Scammers pose as high-ranking officials from government organisations that oversee telecommunications, investigations, or law enforcement. The criminals will contact the victim via encrypted video or audio conversations and falsely state that the victim's listed bank account or cellphone number has been reported for illicit package shipments, human trafficking, or money laundering. The victims is tricked into sending her family's savings to what seem like "government verification accounts" or "safe court accounts," but are actually cyber syndicates' unverified merchant or mule accounts. She is then subjected to severe psychological isolation, legal threats, and mock police interrogations.

Empirical Analysis of Banking Cybercrimes Targeting Women

There has been a dramatic increase in financial cybercrimes directed on female individuals, according to statistical trends recorded across national cybercrime reporting channels. Information gathered by the Indian Cybercrime Coordination Center (I4C) and the National Cybercrime Reporting Portal (NCRP) both fall under the purview of the Ministry of Home Affairs and provide light on the growing prevalence of online banking fraud.

Banking and investment fraud make up more than 70% of overall portal complaints, and a review of national reporting statistics shows that financial cybercrimes are the biggest category of reported digital offences in India. From 48,335 in 2024 to 76,657 in 2025—a 58.6% year-on-year rise—the total number of cybercrime complaints made by women increased, according to NCRP statistics. This increase was more pronounced for female victims. With a 65.9% rise in the banking industry alone, financial fraud accounts for the vast bulk of these accusations.



Banking and investment fraud make up more than 70% of overall portal complaints, and a review of national reporting statistics shows that financial cybercrimes are the biggest category of reported digital offences in India.

Critical Evaluation of the Legal Architecture: IT Act, 2000 and Bharatiya Nyaya Sanhita, 2023

Financial authorities in India have issued regulatory instructions, updated criminal codes, and specialised cyber laws to combat digital financial crimes perpetrated against women. The Information Technology Act of 2000 (IT Act) and criminal penal laws continue to serve as the principal legislative foundation.

Prosecuting crimes using computers has its legislative roots in the IT Act. Theft of identity is criminalised under Section 66C, which details the penalties for the deceitful or fraudulent use of electronic signatures, passwords, or other identifying characteristics. As the principal allegation against vishing and impersonation fraudsters, Section 66D tackles cheating by personation utilising communication devices or computer resources. Furthermore, corporations and financial intermediaries may be held civilly liable under Section 43A if they do not use and uphold "reasonable security practices" while dealing with SPDI.

When it comes to digital financial fraud that targets women today, nevertheless, the IT Act shows certain structural limits. Despite its reactive nature and absence of gender-sensitive language or specialised protection criteria, the law is mainly designed to deal with issues of unauthorised system access and network breaches. When it comes to deterring organised cyber syndicates, the monetary fines and term penalties outlined in Sections 66C and 66D are often inadequate. Additionally, the Act provides few options for automatic loss recovery or interim victim relief while investigations are underway.

The Bharatiya Nyaya Sanhita, 2023 (BNS)

Substantive criminal law in India will undergo a major overhaul in 2023 when the Bharatiya Nyaya Sanhita supersedes the Indian Penal Code of 1860. Incorporating cyber-enabled offences into the fundamental criminal framework is the goal of the BNS. Cheating via personation is dealt with under Section 319, whereas cheating and dishonestly compelling handover of property are both penalised by Section 318. The most important part is that Section 111 establishes clear punishments for "organised crime," classifying structured criminal enterprises like fraudulent financial networks, cyber fraud syndicates, and phoney contact centers as such. Problems with procedural integration remain despite the BNS's harsher punitive remedies and more expansive definitions of digital offences. Complex digital crimes, which often include social engineering, online impersonation, and quick money transfers, are notoriously difficult for law enforcement to map onto specific provisions of the criminal code.

CONCLUSIONS

Financial inclusion, social mobility, and economic empowerment have all been made possible by the digital banking revolution in India. Nevertheless, these accomplishments are jeopardised by the ongoing problem of cyber financial crime that targets female bank customers. Legislation, regulations, and software designs need to change to accommodate cybercriminals' transition from technological system intrusions to psychological social engineering. To tackle this dilemma, we need to shift from a police-first mentality to one that is proactive and thorough. India can create a fair financial system by enforcing existing laws (such as the IT Act and the BNS), implementing protections for intelligent banking interfaces, constructing an enforcement infrastructure that takes gender into account, and encouraging practical digital financial literacy. Ensuring the safety of female residents' digital assets is not only required by law, but also lays the groundwork for maintaining confidence and fairness in the digital economy.

REFERENCES:

1. Indian Cybercrime Coordination Centre (I4C). (2025). National Cybercrime Report. Ministry of Home Affairs, Government of India.
2. Khera, P., et al. (2021). Gender disparities in digital access in rural India. Journal of Development Studies, 57(4), 567–589.
3. Kumar, A. (2020). Challenges in enforcing cyber laws in India. Indian Journal of Criminology, 45(2), 112–130.
4. Reserve Bank of India (RBI). (2023–2025). Master Directions on Fraud Risk Management in Commercial Banks.