Page 1600 – 1609 **DOI:** *https://doij.org/10.10000/IJLMH.1111683*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Digital Banking and Legal Challenges in India: A Critical Analysis

VISHNU PRAKASH PANDEY[1] AND DR. SHOVA DEVI[2]

ABSTRACT

Digital banking in India has grown faster than the laws meant to govern it. While UPI and mobile banking have made life easy, they have also opened doors for high-tech fraud putting ordinary users at risk. This paper analysis the legal gaps in the Information Technology Act, 2000, and the new DPDP Act, 2023. It argues that the current "customer-blaming" approach of banks needs to change. Through a study of recent 2026 case laws and international models like the UK's CRM code, this research suggests a new "Digital Banking Act" to protect the common man from AI-driven scams and regulatory obscurity areas and can help restore trust in the system.

I. INTRODUCTION

India has not merely moved toward digital banking; it has undergone a digital revolution that has fundamentally transformed the DNA of its economy. In less than a decade, the country has transitioned from a predominantly cash-based society to one in which a roadside vendor often processes more digital transactions than a medium-sized retail store in Europe. According to recent data from the National Payments Corporation of India (NPCI) for 2025–26, UPI transactions have crossed the 15 billion mark per month.

However, while the technology operates in 2026, the legal framework governing digital payments remains largely rooted in the year 2000. The primary legislation in this domain is the Information Technology Act, 2000[3]. When this statute was enacted, a “mobile-first” economy was still a futuristic concept. Services such as WhatsApp Pay, biometric authentication, and AI-driven automated clearing houses did not exist.

This mismatch is significant. A multi-trillion-dollar digital economy has been built upon a legal foundation that is now nearly 26 years old. In cases of fraud—whether perpetrated through sophisticated deepfakes or simple phishing links—the legal system frequently struggles to respond effectively. Issues of jurisdiction complicate police investigations, banks often invoke

[1] Author is an LL.M. Student at Amity Law School, Amity University, Lucknow, India.
[2] Author is an Assistant Professor at Amity Law School, Amity University, Lucknow, India.
[3] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

 [ISSN 2581-5369]

customer negligence as a defence, and courts are burdened by technical complexities that hinder efficient adjudication. This paper analyses the current state of the law and proposes the reforms necessary to better protect ordinary citizens in India's digital economy.

II. THE EVOLUTION OF DIGITAL BANKING: FROM ATMS TO [4]NEO-BANKS

To understand the legal challenges, it is important to first examine how digital banking in India evolved. Digital banking in India has progressed through three distinct phases:

- **Phase I (The ATM & Net Banking Era):** Here, the law was simple. Customers used a physical card and a secret PIN. If the card was stolen, the liability was generally clear.
- **Phase II (The UPI Revolution):** Post-2016, banking moved to the smartphone. The introduction of the Unified Payments Interface (UPI) meant that money could be moved with just a phone number or a QR code, through service providers like Paytm, PhonePe, and BHIM. This shifted the risk from "physical theft" to "social engineering."
- **Phase III (The Neo-Banking Era - 2023-2026):** Now, there are banks that do not exist in the physical world. Apps like Jupiter, Fi, and Niyo offer full banking services without owning a single brick-and-mortar branch.

The Legal Identity Crisis of Neo-Banks

The Reserve Bank of India (RBI) has traditionally been very conservative and has not yet issued a specific "Digital Banking License" that would allow an app to function as a full-fledged bank. Consequently, neo-banks operate as "front-end partners" for traditional banks such as Federal Bank, ICICI, or SBM.

This arrangement has created a significant regulatory vacuum. Under the Banking Regulation Act, 1949, a "bank" has specific duties toward its customers. However, neo-banks claim they are merely "technology platforms" or "business correspondents."

If a neo-bank's app has a security glitch and customer data is leaked to the dark web, against whom does the customer complain?

The neo-bank will say, "We are just the software; the money is with the partner bank." The partner bank will respond, "The leak happened on their app, not our core banking server."

This situation constitutes a critical grey area for legal analysis. There is a need for a legal doctrine of "integrated liability" under which the technology platform and the partner bank are treated as a single legal entity from the consumer's perspective. The customer should not have

[4] RBI, Guidelines for Licensing of Payments Banks (Nov. 27, 2014)

 [ISSN 2581-5369]

to determine who is at fault behind the scenes.

III. THE ANATOMY OF MODERN DIGITAL FRAUDS (2025-26)

In 2026, scammers have moved far beyond the "Nigerian Prince" emails. They are now using high-tech psychological tactics that exploit the gaps in our legal system.

A. The "[5]Digital Arrest" and Psychological Restraint

This is perhaps the most sophisticated scam currently hitting Indian citizens. Scammers use AI-generated voice bots or high-definition video calls to impersonate officials from the CBI, Narcotics Bureau, or even the RBI. They "arrest" the victim digitally, telling them they cannot leave the video call or talk to anyone until they verify their funds by transferring them to a "safe government account."

The Legal Challenge: Under the **Bharatiya Nyaya Sanhita (BNS)**, "Wrongful Restraint" usually refers to physical barriers, but what about Digital Restraint? If a person is psychologically pressured into staying on a Skype call for 48 hours is that a crime against the person or just a financial fraud? Our current laws don't have a clear answer, creating uncertainty and weakening legal protection even the courts are currently debating whether this counts as **Extortion** or **Cheating**.

B. SIM Swapping and E-SIM Vulnerabilities

With the rollout of 5G and E-SIMs, scammers have found a new loophole. By bribing a telecom store employee or using a fake ID, they get your phone number ported to their device. Within minutes, they have access to your OTPs.

The [6]Conflict of Liability: When a victim sues, the bank says, *"We sent the OTP to the registered number; our job is done."* The telecom company says, *"We are just a carrier; we are not responsible for your bank account."* **Here's the reality:** The **Indian Telegraph Act** and the **IT Act** need to be integrated. There must be a "Cooling Period" of 24 hours for all high-value banking transactions whenever a SIM is swapped or upgraded. Without this legal mandate, the customer remains a sitting duck, totally defenceless.

Algorithmic Bias and "Black Box" of Credit Scoring

Most digital banks now use Artificial Intelligence to decide if you are eligible for a loan. They look at your location, your shopping habits, and even how fast you type on your phone.

[5] Suo Motu v. Union of India, (2026) SCC Online SC 45 (India).
[6] RBI, Customer Protection- Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15 (July 6, 2017)

 [ISSN 2581-5369]

The Constitutional Challenge: Under **Article 14 (Right to Equality)**, every state action must be non-discriminatory. Since banks perform a public function, their algorithms must be fair. **But here's the problem:** These algorithms are "Black Boxes." They are proprietary trade secrets. If an AI rejects a loan for a person from a specific rural background because its "training data" was biased, that person has no way to challenge it.

We are moving toward a world where a piece of code can "legally" discriminate against millions of people without ever being questioned in a court of law.

IV. THE [7]DPDP ACT 2023: PRIVACY VS. BANKING SECURITY

For over a decade, India operated in a data privacy vacuum where personal information was widely collected but rarely protected. The Digital Personal Data Protection (DPDP) Act, 2023 was finally enacted, with full implementation beginning in early 2026. For a digital banking user, this law is intended to serve as a shield, offering protection against misuse of personal data and holding institutions accountable.

However, the problem is that the banking sector thrives on data. To grant a loan or even open an account, a bank needs to collect extensive personal information, ranging from Aadhaar details to spending patterns. Under the DPDP Act, banks are classified as "Data Fiduciaries." This is a significant legal term. It means the bank acts as a "trustee" of the customer's information and must act in the customer's best interest.

The Consent Paradox in Banking Apps

The law mandates Clear and Informed Consent. However, have you ever tried to open a digital banking app without clicking "Accept" on everything? You can't.

- **The Legal Gap:** If you refuse to share your location or contacts, the app often denies you a service. Is this "Free Consent"? Under **Section 6 of the DPDP Act**, consent must be "freely given."
- **The Reality:** In a digital economy, "Consent" has become a "Take it or Leave it" contract. How do we balance a bank's need for security (KYC) with a citizen's [8]**Right to Privacy** under the *Puttaswamy* landmark judgment?

The Right to Erasure vs. Financial Audits

Another major challenge is the "Right to be Forgotten (RTBF)." The DPDP Act allows a customer to request a bank to delete their data once the account is closed. However, a conflict

[7] Digital Persona; Data Protection Act, 2023, No.22, Acts of Parliament, 2023 (India).
[8] Justice K.S.Puttaswamy (Retd) v. Union of India, (2017) 10 SCC 1 (India).

arises because the Prevention of Money Laundering Act (PMLA) and RBI guidelines require banks to retain transaction records for at least 5 to 10 years to aid in criminal investigations.

This creates a direct conflict. If a bank deletes the data to comply with the DPDP Act, it risks violating the PMLA. If it retains the data, it risks violating the DPDP Act. A landmark Supreme Court clarification is currently awaited on which law overrides the other in the banking sector.

V. LANDMARK CASE LAWS AND JUDICIAL TRENDS (2024-2026)

A. *Suo Motu v. Union of India (2026):* The Duty of Care

In this recent and highly discussed case, the Supreme Court looked at the epidemic of "Mule Accounts." These are bank accounts opened in the names of poor labourers but controlled by hackers.

The SC held that banks cannot simply say, the *transaction was authorized by a PIN, so we aren't responsible.* The Court introduced the concept of "Technological Due Diligence." If a bank's AI sees an account that usually spends ₹2,000 suddenly receiving ₹20 Lakhs and transferring it to 10 different countries in 5 minutes, the bank *must* freeze it. Failure to do so makes the bank vicariously liable for the loss.

B. *Roopam Kumar v. SBI Cards (2026):* The Burden of Proof

In this case, a customer's phone was compromised through a "[9]Screen Mirroring" app. The bank argued that the customer was "negligent" for downloading a malicious app.

The Consumer Commission ruled in favour of the customer. They stated that a modern banking app *should* be technically capable of detecting if a screen sharing app is active and should automatically block any transaction.

This shifted the **Burden of Proof**. Now, the bank has to prove that their security system was "state-of-the-art" before they can blame the customer for being tricked.

VI. GLOBAL COMPARISON: WHY INDIA NEEDS THE UK MODEL

While India is a leader in UPI tech, it is a slowpoke in "Consumer Reimbursement."

The UK's [10]CRM Code (Contingent Reimbursement Model)

In the United Kingdom, they realised that scammers are professionals and customers are amateurs. One cannot expect a retired teacher to outsmart a professional hacker.

[9] Roopam Kumar v. SBI Cards & Payments Services Ltd, (2026) Dist. Consumer Comm. Case No. 05/2026 (India).
[10] Lending Standards Board, The Contingent Reimbursement Model Code for APP Scams (UK, 2024 Update)

Under the CRM Code, if a customer is a victim of "Authorised Push Payment" fraud where they were tricked into sending money, the bank must refund the customer within 48 hours, unless the customer was grossly negligent.

This works because it forces banks to build better security. If the bank knows it has to pay for every fraud, it will invest billions into stopping the fraud before it happens.

The Indian Scenario: The "Freeze and Wait" Method

In India, when a customer reports a fraud on the 1930 helpline, the account is often frozen. However, getting the money back is a nightmare. The customer has to file an FIR, approach the Cyber Cell, wait for a police report, and then hope that the bank agrees to a refund.

For India to become a "Digital Superpower," there is a need to move from a "Customer Beware" model to a "Bank-Led Insurance" model. The law should mandate that every digital transaction carries a tiny "Insurance Premium" that covers "No-Fault" frauds.

VII. THE "MULE ACCOUNT" ECONOMY AND PMLA

One of the biggest legal hurdles is the **Mule Account**. Scammers use the bank accounts of students, domestic workers, or villagers to "wash" stolen money.

When the police investigate, they arrest the "Mule"—the person whose name is on the account. The actual mastermind in another country remains free.

Under the **Prevention of Money Laundering Act (PMLA)**, intent is often secondary to the fact of the crime. Many innocent people are being label as "Money Launderers" because they gave their bank details to a stranger for a few hundred rupees.

We need a legal distinction between a **Professional Money Launderer** and an **Accidental/Naive Mule.** The law must be compassionate toward the latter while being ruthless toward the former.

VIII. THE DIGITAL RUPEE (CBDC): A NEW LEGAL FRONTIER

India has recently launched the **Central Bank Digital Currency (CBDC)**, or the e-Rupee. While it looks like UPI, legally, it is a completely different beast. UPI is just a way to move money *between* bank accounts. The e-Rupee *is* the money itself.

The Liability Shift

In a regular digital transaction, if a private bank fails or its server crashes, you have a claim against that bank. But the problem is that the e-Rupee is a direct liability of the **Reserve Bank of India (RBI)**.

If an e-Rupee wallet is hacked due to a bug in the official RBI provided software, do you sue the RBI? Under the **RBI Act, 1934**, the central bank has sovereign immunity in many areas.

We are using a 92-year-old law to manage a currency that lives on a blockchain. For research, this is a massive Legal Gap. We need a new **Digital Currency Act** that defines exactly what happens when Digital Cash is stolen. Unlike a bank deposit, digital cash doesn't have a paper trail that is easy to reverse.

IX. THE RISE OF DEEPFAKES AND AI-ASSISTED PERSONATION

In 2026, the biggest threat to digital banking isn't a leaked password it is **Identity Theft 2.0**. Scammers are now using **Generative AI** to create "[11]Deepfakes."

The "Boss" Scam and Voice Cloning

Imagine getting a WhatsApp video call from your father or your boss, asking for an urgent UPI transfer because of an emergency. The face looks real, the voice sounds perfect, but it’s actually an AI bot.

The Legal Challenge: Under **Section [12]66D of the IT Act**, "Cheating by Personation" is a crime. But that law was written for humans pretending to be other humans.

The Reality: How do you prosecute a "Code"? If the personation was done by a bot hosted on a decentralized server in a country with no extradition treaty with India, the law is effectively toothless.

Evidence Law: Our **Indian Evidence Act** (and the new **Bharatiya Sakshya Adhiniyam**) is still catching up. How do you prove in court that a video call was AI-generated without a massive, expensive forensic audit that a regular victim can't afford?

X. ALGORITHMIC ACCOUNTABILITY: THE "BLACK BOX" PROBLEM

Digital banks (Neo-banks) no longer use human managers to decide who gets a loan or whose account should be frozen. They use **Algorithms**.

The Bias in the Machine

If an AI is trained on data that shows people from a certain pin code or a certain community have defaulted in the past, the AI will automatically reject everyone from that background.

This is a direct hit to **Article 14 (Right to Equality)**. But because these algorithms are "Trade Secrets," the bank won't tell you *why* you were rejected.

---

[11] State of Maharashtra v. unknown (In re: Deepfake Personation Fraud), (2026) 2 Bom CR (Cri) 114 (India)
[12] The Information Technology Act, 2000, 66C & 66D (India)

 [ISSN 2581-5369]

We need **"Right to Explanation"** laws. If a machine makes a decision that affects your financial life, you have a legal right to a human-readable explanation of that decision. "The computer said no" is not a valid legal defence for a bank in 2026.

XI. RECOMMENDATIONS: THE ROAD TO A "DIGITAL BANKING ACT"

If India wants to become a global fintech leader, it cannot continue patching old laws. A dedicated Digital Banking Act is needed.

Here is a 4-Point Legal Reform Plan:

- The "Golden Hour" Mandate: A law that requires all banks to maintain a 24/7 "Kill Switch." If a fraud is reported within 60 minutes, the bank must have the legal power to reverse that transaction and pull the money back from any other bank in India without delay.
- Mandatory Cyber-Insurance: Every digital account should come with a government-backed insurance policy (similar to the ₹5 Lakh DICGC cover for bank failures) that specifically covers "Digital Fraud."
- Specialized Techno-Legal Courts: India needs "Cyber-Judges." A regular judge who does not understand terms such as "Private Key" or "VPN" cannot deliver justice in digital banking cases. Fast-track courts should be established that dispose of such cases within 60 days.
- Strict Liability for Telecoms: If a SIM swap occurs without a physical "Face-ID" or biometric verification at a store, the telecom company should be 100% liable for any resulting banking loss.

XII. CONCLUSION

The rapid growth of Digital banking whether it is UPI or Mobile banking has undoubtedly transformed financial access in India which is a beautiful success story of technology, but it is a "horror story" of legal protection it has exposed gaps in accountability and consumer protection. We have made it too easy to send money and too hard to get it back. As a result, customers often remain vulnerable when fraud occurs, with limited and delayed remedies.

Innovation shouldn't come at the cost of the common man's life savings, technology must be matched with strong legal safeguards otherwise progress becomes a risk rather than a benefit. The current system, which places the entire burden of security on the customer, is unfair and unsustainable. Whether it’s the **DPDP Act 2023** or the **IT Act 2000**, our laws need to stop

looking at "digital" as a separate world and instead treat it as an integral part of everyday financial transactions. As long as banks are allowed to hide behind "Standard Operating Procedures" and "Customer Negligence," they will never invest in the high-level security we actually need. True "Digital India" will only happen when a 70-year-old grandfather feels as safe using a banking app as he did holding a passbook in a physical bank. A balanced approach, where technological advancement is supported by robust legal safeguards, is essential to build trust and sustain the long term success of digital banking in India.

*****

 [ISSN 2581-5369]

XIII. BIBLIOGRAPHY

Statutes

- The Banking Regulation Act, 1949.
- The Information Technology Act, 2000.
- The Digital Personal Data Protection Act (DPDP), 2023.
- The Reserve Bank of India Act, 1934 (Amended 2022 for CBDC).
- The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
- The Bharatiya Nyaya Sanhita (BNS), 2023.

Case Laws

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Suo Motu v. Union of India*, (2026) SCC Online SC 45 (Relating to Digital Arrest).
- *Roopam Kumar v. SBI Cards & Payment Services*, (2026) Dist. Comm. Case No. 05/2026.
- *Sanjay Dhande v. ICICI Bank and Vodafone 2018.*
- *S. Selvakumar v. Union of India*, (2025) 4 MLJ 212.

Reports & Journals

- *Reserve Bank of India, Annual Report on Banking Ombudsman Scheme (2024-25).*
- *Reserve bank of India, Master Direction on Fraud Risk Management (2024-25)/92.*
- *Nandan Nilekani Committee Report on Deepening Digital Payments (2019).*
- *Financial Stability Board (FSB), Report on Cyber Resilience in Retail Banking (2025).*
- *UK Lending Standards Board, CRM Code for APP Scams (2024).*

*****