



## Digital Payment Frauds in India: Role of Banks and Legal Protection for Consumers

Y. Papa Rao, Ph.D., Pratiksha Pal, LL.M, Department of Law  
Hidayatullah National Law University, Raipur, Chhattisgarh, INDIA

### ORIGINAL ARTICLE



### Authors

Y. Papa Rao, Ph.D.  
Pratiksha Pal, LL.M

E-mail : dr.yamala@hnlu.ac.in

shodhsamagam1@gmail.com

Received on : 15/07/2026  
Revised on : 16/09/2026  
Accepted on : 26/09/2026  
Overall Similarity : 06% on 18/09/2026



### Plagiarism Checker X - Report

Originality Assessment

**6%**

Overall Similarity

Date: Sep 18, 2026 (01:34 PM)  
Matches: 169 / 2782 words  
Sources: 12

Remarks: Low similarity detected, consider making necessary changes if needed.

Verify Report:  
Scan this QR Code



### ABSTRACT

Digital payment fraud in India sits at an odd crossroads. The country's push for financial inclusion through Aadhaar and UPI has been remarkable, over a billion biometric identities linked to a payment system processing roughly 1.7 trillion transactions by 2023. Yet the legal machinery meant to protect users has lagged well behind this growth. This paper examines that gap through a close reading of RBI's 2017 Customer Protection circular and three contrasting judicial decisions. In *Suresh Chandra Singh Negi v. Bank of Baroda*, the Allahabad High Court sided with the bank after login logs revealed the customer's own culpability. *Hare Ram Singh v. RBI* told a different story: a Delhi court held SBI liable for delayed action after a phishing scam, setting a demanding threshold for what counts as customer negligence. Taken together, these rulings show how much depends on timing, on how quickly a victim reports fraud, and on whether courts view the customer as reckless or merely unlucky. The paper argues that India's current model, which still leans heavily on consumer vigilance and the notice-and-consent framework, asks too much of ordinary users navigating cognitively demanding digital environments. Legal certainty around virtual assets remains an unresolved thread worth pursuing separately.

### KEY WORDS

Digital Payment Fraud, RBI Customer Protection Circular, Bank Liability, Upi, Consumer Protection Law, Virtual Assets Regulation.

### INTRODUCTION AND BACKGROUND

Over the last several years, India has experienced a radical digital revolution in the sphere of financial operations, which is, to a large extent, driven by a national push towards financial inclusion. Although this has brought about a great deal of convenience and

efficiency, it has also created a complicated system of environment in which fraud is likely to occur and this is a major challenge to both consumers, financial institutions, and regulators. The current report explores online payment fraud in an Indian situation, providing a study of the current legal and regulatory system, liability of financial institutions and efficacy of consumer protection systems.

The digital economy in India is supported by a complex Digital Public Infrastructure (DPI), informally called the India Stack, an interoperable government-supported ecosystem that is meant to simplify the interaction between people, businesses, and government bodies. At the core of this infrastructure is the Aadhaar authentication system that has issued biometrics identifiers to more than 1.3 billion citizens, thus allowing them to be verified quickly and securely. As a complement to Aadhaar, the Unified Payments Interface (UPI), an open-ledger payment system, enables digital transactions with the lowest friction and, therefore, eliminates any ancillary expenditure on both sides.

One of the most obvious examples of fraud is the so-called Digital Arrest scam, where fraudsters fake leadership roles in the government to manipulate victims into paying money, using the false accusations of KYC failures or other alleged financial offenses.

The rising rate and complexity of these frauds demonstrate the high urgency of the development of a legal framework that will be updated with the changing levels of technology.

## **The Regulatory and Statutory Framework in India**

### **Overview of the Digital Public Infrastructure (DPI) and its Governance**

The India Stack is the foundation of the digital economy in India, but it is organized into three major layers<sup>1</sup>; the ID layer, the payment layer and the data layer. The ID layer which is driven by Aadhaar system gives a unique biometric identity to about 1.3 billion citizens so that the instant verification of identity is done in a broad spectrum of services. The payment layer is developed with the Unified Payments Interface (UPI)<sup>2</sup> which is an open digital payment system that has revolutionized financial transactions in India. As of 2023, UPI digital transactions were being processed in volume of about 1.7 trillion<sup>3</sup> representing over a third of digital retail transactions in the country. The third tier is the data layer and the platform involved in this layer is the DigiLocker which enables individuals to store and share personal information securely containing tax records, educational certificates, and medical documents.

This ecosystem is managed in a complex manner, touching upon the government control, the non-governmental organizations (NGOs)<sup>4</sup>, and the partnership of the government and businesses. Although this multi-stakeholder model has made it possible to gain rapid growth and extensive use, it has brought serious challenges. The rapid implementation of the Digital Public Infrastructure (DPI) driven by the aspiration of the financial inclusion has progressed far ahead of the construction of a proactive and versatile regulatory framework. Consequently, the laws and other regulatory measures that ensure the security of this infrastructure have not kept up well with the advancement in technology. This weakness leaves the cybercriminals with a loophole through which they can exploit weaknesses before the law gets to adapt<sup>5</sup>.

### **Key Regulatory Bodies and their Jurisdictions**

A number of regulatory authorities are involved in managing the cases of digital payment frauds and the mandates may tend to overlap and need close coordination of their functions. The central bank of India (RBI) is the main authority of the control of the banking and payment systems<sup>6</sup>. Its circulars and guidelines especially those that deal with Customer Protection are the foundation of ascertaining the liability of a bank in electronic transactions. Meanwhile, a lot of frauds are committed or enabled by telecommunications networks. The Telecom Regulatory Authority of India (TRAI), the regulator of this sector, has circulated public warnings to the citizens against fraudulent schemes in the industry like Digital Arrest schemes and fake mobile towers installation schemes, which misuse its name.

The involvement of various agencies working under their jurisdiction and regulating environments<sup>7</sup> is a manifestation of the multi-agency and multi-jurisdictional prerogative of the issue of digital fraud. In this regard, the coordination and combined efforts of the regulators must also be effective as a measure to prevent and curb such frauds.

## **The Legal Status of Virtual Assets and its Implications**

The legal status of virtual assets in India has been the centre of the heated debate, which is one of the obvious examples of the legal system making attempts to change. Reserve Bank of India (RBI) had issued warnings in 2013 and 2017, which has culminated in a blanket ban on virtual currency transactions in 2018. The RBI explained this action by citing money laundering and financing of terrorism as some of the risks<sup>8</sup>. Nevertheless, in 2020, it was ruled by the Supreme Court that the ban could be lifted, thus paving the path to a new method of regulation.

In 2022, the Indian government made its stance clear by not accepting virtual assets as legal money instead of a harsh taxation regime. Under the Union Budget FY 2022-23, the taxes levied on income earned through virtual assets were 30 percent and on transactions was 1 percent Tax Deducted at Source (TDS). This payment in terms of taxation model although appreciating the existence of virtual assets has resulted in a conflicting regulatory environment. On the one hand, the government actively stimulates the development of blockchain, the most significant of which is the proposed establishment of the so-called Digital Rupee a Central Bank Digital Currency (CBDC)<sup>9</sup>. Conversely, it is still unclear in the legal context of private virtual assets.

Even though taxation makes virtual assets viable as a source of revenues, the lack of a definite and elaborate legal framework means that the investor is left vulnerable and has little means of suing in court or during cases of consumer disputes<sup>10</sup>. This fact begs the core issue of whether the existing framework actually does exist to safeguard consumers or is more aimed at monopolizing the digital economy- this may be at the cost of consumer protection. Even though taxation makes virtual assets viable as a source of revenues, the lack of a definite and elaborate legal framework means that the investor is left vulnerable and has little means of suing in court or during cases of consumer disputes.<sup>11</sup>

## **The Role of Banks, Ppis and The Principle of Liability**

### **The “Customer Protection” Circulars as the Cornerstone of Liability**

Majority of the liability frameworks of the unauthorized electronic banking transactions in India are influenced by the Reserve Bank of India (RBI) circular dated July 6, 2017, entitled Customer Protection-limiting Liability of Customers in Unauthorised Electronic Banking Transactions. The prominent aspect of this model is that the firm dealing with the liability of a customer in instances where wrong transactions have been executed is placed on the bank. The circular identifies some situations where the customers can claim zero liability. This is applicable in such instances as third-party breach where the bank and the customer are not to blame as long as the customer reports to the bank within three working days.<sup>12</sup>

This principle has the aim of protecting consumers against the effects of systematic vulnerabilities in the digital payment system and to hold banks responsible to have adequate transaction systems in place.

## **Judicial Interpretation of Liability and Negligence: A Case Law Analysis**

### **Case 1: Suresh Chandra Singh Negi v. Bank of Baroda (Allahabad High Court).**

Facts: These two businessmen would have approached the court claiming that 38.78 lakh should be returned by the court because it was fraudulently stolen out of their accounts. The Bank of Baroda though argued that the transactions were not fraudulent. When the court reviewed the debit/credit records, and the lists of IP addresses, they established that the petitioners themselves conducted the transactions by accessing their internet banking account, which had created One-Time Passwords (OTPs) and had inserted the beneficiaries.<sup>13</sup>

Result(s) & Reason: The Allahabad High Court rejected the petition and ruled that the petitioners had been grossly negligent. The court established that the transactions were not accidental and that the statements given by the petitioners were a made-up account whose aim was to make personal dealings look like cyber fraud. The bank managed to overcome the burden of proving its guilt by demonstrating logs of logins, change of passwords and OTPs.

This case demonstrates that although the burden of proving should be on banks in the first instance with the framework of RBI this does not mean that it is unreliable. Courts will not assist those customers who are determined to be complicit or grossly negligent in their personal transactions.

### **Case 2: Hare Ram Singh v. Reserve Bank of India (Delhi high court).**

Facts: An academician lost 2.6 lakh after opening a fake link sent by an unknown telephone caller. The funds were redirected in two transactions one to an account of the Paytm and the other account of the IDFC Bank. The petitioner instantaneously communicated with the customer care of SBI to block the transactions and also lodged a complaint with police. Nevertheless, SBI did not act on time.<sup>14</sup>

Outcome & Rational: Delhi High Court ruled that SBI was responsible of the loss, and ordered the bank to pay the petitioner with interest. The court saw the petitioner as a victim of an advanced cyber fraud and not a careless customer since he had not provided his OTPs. Notably, the court has established the high standard of proving the presence of negligence on the part of the customer, which must be characterized as gross, utter recklessness, and unconscionable.

The court also highlighted that banks owe a standard of care of reasonably acting and taking immediate action when they suspect fraud. SBI was determined to be wanting in its service concerning the failure to initiate a chargeback or freeze the suspicious accounts as soon as possible. The court further condemned the misinterpretation of the law by the Banking Ombudsman, which was a major drawback of the redressal system of regulations.

## **Legal Protection and Redressal Mechanisms for Consumers**

### **The Consumer Protection Act, 2019: A New Dawn?**

The Consumer Protection Act, 2019 (CPA, 2019)<sup>15</sup> was enacted to eliminate the weaknesses of the previous 1986 Act, particularly in light of the emergence of online commerce.

The most significant changes introduced under CPA, 2019, mediation as an Alternative Dispute Resolution (ADR) mechanism should be mentioned. The Act provides Consumer Mediation Cells to the consumer commissions at the district, state, and national levels. This is a mechanism that is meant to offer a quicker and more affordable way of conflict resolution.

### **The Challenge of John Doe Defendants and Digital Redress**

Anonymity is inherent with the internet and this greatly hinders identification and subsequent prosecution of cybercriminals. This is especially a challenge when dealing with the John Doe defendants where the identity of a perpetrator is unknown. A good example of this obstacle is the judicial proceeding Razorpay Software (P) Ltd. v. John Doe. In this case, the participants were involved in personifying the Razorpay brand to perpetrate a financial fraudulent scheme. They created fake websites with domain names that were similar to the one owned by the legitimate party, duplicated the company user interface and used forged legal papers to give it an air of legitimacy.

### **The Inadequacy of Public Awareness as a Sole Strategy**

While advisories from regulatory bodies like TRAI play an important role in warning the public about emerging scams, a legal system that relies only on consumer education and vigilance is deeply inadequate. Academic studies of consumer behavior show that the “notice and consent” model does not work effectively in today’s digital markets. Consumers are not fully rational decision-makers; they face cognitive biases, time pressures, and information overload, which make it difficult to properly assess risks.

As a result, placing the main responsibility on consumers to stay alert is not a sufficient strategy against sophisticated and well-funded cybercriminal networks. These limitations should be considered by a stronger legal framework and the responsibility should be redirected at creating a safe digital ecosystem.

## **CONCLUSION/FINDINGS**

### **Findings**

- **The Reactive Regulatory Landscape:** Regulatory responses in the past have been reactive and regulators and the government would only respond to technological shifts once they become commonplace or cause considerable legal debate. This reactive approach has given rise to a patchy and unpredictable state of regulation and has exposed not only the consumer but also the investor to increased risk.

- **Dependent on facts of the Judiciary:** The distribution of liability in fraud situations is very fact-finding. The judicial rulings depend on the fact that a customer acts as a victim or a negligent party. These two cases though showing divergent results indicate that the burden of proof rests with the bank but it is the consumer whose complaint and timing would play a key role in deciding on the liability.
- **Greater Exposure to Non-Banked Entities:** Among the significant changes is the ease with which the judiciary has been ready to impose liability on non-bank issuers that provide payment services, including Paytm. This change is an indication of willingness to transform consumer protection principles to the dynamic digital-payment environment, and thus increase equity and safety in financial services.
- **The Flawed Consumer Diligence Model:** Existing consumer-oriented approaches, which are based on awareness and vigilance, put an unnecessary burden on people and make them responsible. The model of notice-and-consent, specifically, does not work well in online situation because it does not take into consideration cognitive and practical obstacles a consumer may encounter.

## Suggestions

- **Revision of Proactive, Substantive Regulation:** Regulators should no longer engage in a reactive approach to regulation, but instead adopt a new paradigm that is proactive through the embrace of substantive controls and mandatory standards. Rather than continuing with the notice-and-consent strategy that has been proven to be ineffective, regulators ought to foresee the upcoming challenges and come up with clear-cut, enforceable provisions that deal with digital security, data protection and the terms of the contract.
- **Enhanced Banking Privacy and Prevention of Liability:** Banks should not be the sole bearers of the responsibility to ensure that they verify the behaviour of their customers but also prove that they have sufficient security infrastructure. Furthermore, legal definition of customer negligence must be enshrined at a very high standard like gross or unconscionable recklessness to avoid absolving institutions of liability in the event of advanced cyber-attacks.
- **Establish a Common Centralized Digital Redressal Repository:** The government must establish a digital redressal application to become a one-stop venue to victims of fraud that is in accordance with the Consumer Protection Act. This national portal should be connected with law-enforcement agencies, National Cybercrime Helpline and Consumer Mediation Cells. Such a system would minimize the bureaucratic stalling, speed up the speed of dispute resolution and make consumer reporting to be reciprocated by an immediate institutional response.
- **Virtual Asset Legal Certainty:** There should be a detailed legal system of rights and obligations and measures of dispute resolution that would protect investors and at the same time encourage technological innovation.

## REFERENCES

1. Cambridge University Press, Cambridge Global Handbook of Financial Infrastructure: India (2025). available at <https://www.cambridge.org/core/books/cambridge-global-handbook-of-financial-infrastructure/india-stack/C1F95AE504C301C88BB3BFE796D220DB>, Accessed on 21/04/2026.
2. Systemic Risk Centre, Digital Infrastructure and Systemic Risk (Discussion Paper No. 131, Feb. 2025). available at <https://www.systemicrisk.ac.uk/sites/default/files/2025-02/DP-131.pdf>, Accessed on 10/05/2026.
3. World Bank, Indias Digital Transformation Could Be a Game-Changer for Economic Development (2025). available at <https://blogs.worldbank.org/en/developmenttalk/indias-digital-transformation-could-be-game-changer-economic-development>, Accessed on 10/05/2026.
4. Agustín González-Agote, Indias DPI Success: A Global Blueprint, IE Insights (2025). available at <https://www.ie.edu/insights/articles/indias-dpi-success-a-global-blueprint>, Accessed on 11/05/2026.
5. Ibid

6. Reserve Bank of India, *Guidance Note on Management of Operational Risk* (2021). available at <https://www.rbi.org.in/upload/notification/pdfs/66813.pdf>, Accessed on 10/05/2026.
7. Carlos Ragazzo & Lucas Caminha, Central Banks as Regulators and (also) Operators of Instant Payments Schemes: Confronting the Criticisms of “Needless Intervention” and “Unfair Competition”, 16 *Eur. J. Risk Reg.* 1 (2025). available at <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/central-banks-as-regulators-and-also-operators-of-instant-payments-schemes-confronting-the-criticisms-of-needless-intervention-and-unfair-competition/FFB46F78BFAF5299806C8B0A27793275>, Accessed on 11/05/2026.
8. Supra Note 6
9. Supra Note 7
10. Systemic Risk Centre, *Digital Infrastructure and Systemic Risk* (Discussion Paper No. 131, Feb. 2025). available at <https://www.systemicrisk.ac.uk/sites/default/files/2025-02/DP-131.pdf>, Accessed on 11/05/2026.
11. Supra Note 3
12. Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (July 6, 2017), available at [https://www.netbanking.indianbank.in/jsp/RBI\\_Limited\\_Liability\\_Policy.pdf](https://www.netbanking.indianbank.in/jsp/RBI_Limited_Liability_Policy.pdf), Accessed on 15/05/2026.
13. *Suresh Chandra Singh Negi v. Bank of Baroda*, Writ (C) No. 24192/2022 (All. H.C. July 17, 2022).
14. *Hare Ram Singh v. Reserve Bank of India & Ors.*, W.P. (C) No. 13497/2022 (Del. H.C. Sept. 16, 2022).
15. The Consumer Protection Act, 2019, No. 35 of 2019, Acts of India § 1 (India), <https://consumeraffairs.nic.in/sites/default/files/Consumer-Protection-Act2019.pdf>, Accessed on 11/05/2026.

\*\*\*\*\*