# LEGAL ISSUES IN DIGITAL PAYMENTS AND CONSUMER PROTECTION IN INDIA

Likitha M, JSS Law College, Mysuru
M C Usharani, JSS Law College, Mysuru

## ABSTRACT

The rapid development of digital payment systems has significantly transformed the financial landscape in India.[1] With the growing use of internet banking, mobile wallets, debit and credit cards, and Unified Payments Interface (UPI), consumers increasingly rely on electronic platforms [2]for financial transactions. While digital payment systems enhance convenience, efficiency, and financial inclusion, they also create several legal and regulatory challenges related to cyber security, consumer protection, privacy, and liability for unauthorized transactions. Incidents of online fraud, phishing attacks, identity theft, and data breaches have raised concerns regarding the adequacy of existing legal frameworks in protecting consumer interests. This paper critically examines the regulatory structure governing digital payments in India, including the Payment and Settlement Systems Act, 2007[3], the Information Technology Act, 2000, and the Consumer Protection Act, 2019[4]. The study also analyzes the role of regulatory authorities such as the Reserve Bank of India in supervising digital payment systems. Further, the paper explores emerging legal issues related to fintech companies, data protection, and dispute resolution mechanisms[5]. The article concludes by proposing reforms aimed at strengthening consumer protection and ensuring secure digital financial transactions in India.

**Keywords:** Digital Payments, Consumer Protection, Cyber Fraud, FinTech Regulation, Data Privacy, RBI Guidelines, Unauthorized Transactions, Digital Banking Law.

[1] Nandan Nilekani Committee, Report of the High-Level Committee on Deepening of Digital Payments, Reserve Bank of India (May 2019)
[2] National Payments Corporation of India (NPCI), UPI Product Statistics (2025/2026), available at npci.org.in.
[3] Reserve Bank of India, Master Direction on Digital Payment Security Controls, RBI/2020-21/74 (Updated 2021).
[4] The Consumer Protection (E-Commerce) Rules, 2020 (notified under the 2019 Act).
[5] The Digital Personal Data Protection Act, No. 22 of 2023 (Gazette of India).

## 1. Introduction

The digital revolution has transformed financial systems across the world. In India, digital payment technologies have gained remarkable momentum due to increasing internet penetration, smartphone usage, and government initiatives aimed at promoting a cashless economy[6].

Platforms such as mobile banking applications, digital wallets, and Unified Payments Interface (UPI) have enabled consumers to perform financial transactions quickly and efficiently.

The Government of India has actively promoted digital financial inclusion through initiatives such as the Digital India programme, which encourages citizens to adopt electronic modes of payment. These developments have improved accessibility to banking services, particularly for individuals in rural and semi-urban regions[7].

Despite these advantages, the widespread adoption of digital payment systems has introduced several legal concerns. Consumers frequently encounter risks such as cyber fraud, phishing attacks, unauthorized transactions, and misuse of personal data. These issues highlight the importance of establishing a comprehensive legal framework capable of safeguarding consumer rights while maintaining the efficiency of digital financial services[8].

This paper aims to examine the legal issues associated with digital payment systems in India and evaluate the effectiveness of the existing legal framework in protecting consumers[9].

## 2. Evolution of Digital Payment Systems in India

Digital payments refer to financial transactions that occur through electronic platforms without the exchange of physical currency[10]. These systems rely on technological infrastructure such as internet banking, payment gateways, mobile applications, and electronic cards to facilitate financial transfers.

India's digital payment ecosystem has evolved rapidly over the past decade. The introduction of the Immediate Payment Service (IMPS) in 2010 enabled real-time electronic fund transfers

[6] Reserve Bank of India, National Strategy for Financial Inclusion (NSFI): 2025-2030 (released Dec. 1, 2025).
[7] Press Information Bureau, RBI's Financial Inclusion Index rises to 67 in 2025 indicating Growth for Everyone, Ministry of Finance (Aug. 6, 2025).
[8] Digital Personal Data Protection Rules, 2025, notified by MeitY on Nov. 13, 2025, under the Digital Personal Data Protection Act, 2023.
[9] State Bank of India v. Pallabh Bhowmick & Ors., SLP (Crl.) No. 56800/2024 (Supreme Court of India, Jan. 3, 2025).
[10] https://www.rbi.org.in

between bank accounts[11]. Subsequently, the National Payments Corporation of India introduced the Unified Payments Interface (UPI), which revolutionized digital transactions by enabling instant payments using mobile devices[12].

The demonetization policy implemented in 2016 further accelerated the adoption of digital payment platforms by encouraging citizens to reduce dependence on cash transactions[13]. As a result, digital payment systems such as mobile wallets, QR code payments, and UPI-based applications have become widely used across the country.

While these developments have enhanced financial inclusion and improved economic transparency, the rapid expansion of digital financial services has also exposed consumers to technological vulnerabilities and legal challenges.

## 3. Regulatory Framework Governing Digital Payments in India

### 3.1 Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act, 2007 [14]provides the statutory framework for regulating electronic payment systems in India. The Act empowers the Reserve Bank of India to supervise and regulate payment system operators to ensure the safety and efficiency of financial transactions.

Under the Act, entities operating payment systems must obtain authorization from the RBI before commencing operations. This regulatory mechanism ensures that digital payment service providers comply with prescribed security standards and operational guidelines[15].

### 3.2 Role of the Reserve Bank of India

The Reserve Bank of India serves as the primary regulatory authority responsible for overseeing digital payment systems in the country[16]. The RBI formulates policies and issues guidelines to maintain the stability, security, and efficiency of the payment infrastructure.

Several regulatory measures introduced by the RBI focus on protecting consumers from

[11] National Payments Corporation of India (NPCI), Immediate Payment Service (IMPS): Product Overview, available at [suspicious link removed] (last visited Mar. 11, 2026)
[12] National Payments Corporation of India (NPCI), Unified Payments Interface (UPI) Product Booklet (2016)
[13] *S. Gupta & S. Agarwal, The Impact of Demonetization on Digital Payments in India, 25(3) J. Fin. Stud. 112 (2018).*
[14] The Payment and Settlement Systems Act, No. 51 of 2007, Preamble (India Code)
[15] Reserve Bank of India, Master Direction on Digital Payment Security Controls, RBI/2020-21/74 (Feb. 18, 2021)
[16] Reserve Bank of India, *Master Direction on Issuance and Operation of Prepaid Payment Instruments (PPIs)*, RBI/DPSS/2021-22/82 (Updated Aug. 2025)

unauthorized electronic banking transactions. These measures require banks to implement security features such as two-factor authentication, transaction alerts, and fraud monitoring systems.

### 3.3 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 provides legal remedies to consumers who suffer financial losses due to service deficiencies[17] or unfair trade practices by digital payment providers. The Act recognizes electronic transactions and extends consumer protection to the digital marketplace.

Consumers may approach consumer dispute redressal commissions if they experience negligence or service failures by digital payment platforms, banks, or financial institutions[18].

### 3.4 Information Technology Act, 2000

The Information Technology Act, 2000 plays an essential role in addressing cyber offences associated with digital payment systems. The Act criminalizes activities such as hacking, identity theft, data theft, and online fraud.[19]

Sections of the Act impose penalties for unauthorized access to computer systems and misuse of electronic data. Additionally, the Act recognizes electronic records and digital signatures, thereby giving legal validity to electronic transactions.[20]

## 4. Major Legal Issues in Digital Payments

### 4.1 Cyber Fraud and Phishing Attacks

Cyber fraud has become one of the most significant threats to digital payment systems. Fraudsters frequently use phishing emails, fraudulent phone calls, and fake websites to obtain confidential banking information from consumers. Once such information is obtained, unauthorized transactions may be carried out.

The increasing sophistication of cybercrime requires stronger regulatory oversight and improved cybersecurity measures.[21]

[17] *The Consumer Protection Act, No. 35 of 2019, § 2(11) & § 2(47) (India Code).* Section 2(11)
[18] *Arun Bhati v. HDFC Bank Ltd., (2025) CPJ 142 (NCDRC).*
[19] *The Information Technology Act, No. 21 of 2000, § 66, 66C & 66D (India Code).* Section 66C
[20] Karnika Seth, Computers, Internet and New Technology Laws, (LexisNexis, 2024)
[21] The Digital Personal Data Protection Act, 2023 and The Digital Personal Data Protection Rules, 2025.

### 4.2 Data Privacy and Security Concerns

Digital payment platforms collect and store large volumes of personal and financial data. The misuse or unauthorized disclosure of such data can lead to identity theft and financial exploitation.

The introduction of stronger data protection regulations is essential to ensure that digital payment providers adopt secure data management practices.

### 4.3 Consumer Liability in Unauthorized Transactions

Determining liability in cases of unauthorized electronic transactions is a critical legal issue. According to RBI guidelines, consumer liability may vary depending on the circumstances under which the fraudulent transaction occurred.

If the fraud occurs due to negligence on the part of the bank or payment service provider, the consumer may not be held responsible for the financial loss[22]. However, if the consumer fails to report unauthorized transactions within the prescribed time period, partial liability may arise.

### 4.4 Liability of FinTech Companies and Payment Intermediaries

The growth of financial technology companies has significantly expanded the digital payment ecosystem. FinTech firms provide innovative payment solutions through mobile applications and digital platforms.[23]

However, the legal responsibilities of these intermediaries in cases of fraud, data breaches, or transaction failures remain unclear in certain situations. Establishing clear liability frameworks for fintech companies is necessary to ensure accountability and consumer protection.

## 5. Dispute Resolution Mechanisms

Efficient dispute resolution mechanisms are essential for addressing consumer complaints related to digital payments. The Reserve Bank of India has introduced the Integrated Ombudsman Scheme, which provides consumers with an alternative platform for resolving banking and digital payment disputes.

Under this scheme, consumers can file complaints against banks and payment service providers without the need for lengthy judicial proceedings[24]. The scheme aims to provide

[22] Hare Ram Singh v. Reserve Bank of India, 2024 SCC OnLine Del 8039 (Delhi High Court)
[23] IFSCA (TechFin and Ancillary Services) Regulations, 2025.
[24] The Digital Personal Data Protection Rules, 2025.

faster and more accessible grievance redressal mechanisms for affected consumers.

**Judicial Approach Towards Digital Payment Fraud**

Indian courts have increasingly addressed disputes involving electronic banking fraud and digital payment failures. Judicial decisions emphasize the responsibility of financial institutions to maintain adequate security systems and protect customer accounts from unauthorized access.

Courts have also held banks liable in cases where fraudulent transactions occur due to inadequate security infrastructure or negligence in responding to consumer complaints.

These judicial interpretations have played an important role in strengthening consumer protection within the digital financial sector.

**State Bank of India v. Pallabh Bhowmick & Ors. (2025)**

**Landmark Supreme Court Ruling on Bank Liability**

The decision in State Bank of India v. Pallabh Bhowmick & Ors. is a significant ruling in Indian banking and cyber-fraud jurisprudence. The Supreme Court clarified the liability of banks in cases of unauthorized electronic banking transactions and reaffirmed the "zero liability of customers" principle under the Reserve Bank of India (RBI) guidelines.

The respondent, Pallabh Bhowmick, held a savings account with the State Bank of India (SBI). In October 2021, he attempted to return a product purchased online. Soon after, he received a phone call from a fraudster posing as a customer-care representative of the retailer. The fraudster induced him to download a remote-access application on his mobile phone.

Using this access, the fraudster conducted three unauthorized online transactions totaling ₹94,204.80 from the respondent's bank account. The customer immediately reported the fraudulent transactions to the bank and also filed complaints with the cyber-crime authorities and the police. Despite timely reporting, the bank failed to reverse the transaction or initiate prompt recovery measures.

**Procedural History**

1. The customer approached the RBI Ombudsman, but his complaint was rejected.
2. He then filed a writ petition before the Gauhati High Court, which directed SBI to refund the entire amount to the customer.
3. SBI challenged this order before the Supreme Court by filing a Special Leave

Petition (SLP).

4. The Supreme Court dismissed the SLP in January 2025, thereby upholding the High Court's decision.

**Legal Issues**

The Court considered the following issues:

- Whether the bank is liable for unauthorized electronic transactions carried out through cyber fraud.
- Whether the customer's conduct amounted to negligence.
- Whether RBI guidelines on "zero liability" apply to the case.

**Court's Reasoning**

The Supreme Court held that the transactions were clearly unauthorized and fraudulent, and there was no evidence of negligence on the part of the customer.

The Court emphasized that banks possess advanced technological systems and must ensure the security of customers' accounts. It stated that financial institutions cannot escape liability by blaming third-party applications or fraudsters.

The Court relied on the RBI Circular dated 6 July 2017 on Customer Protection in Unauthorized Electronic Banking Transactions, which provides that:

- If a customer reports an unauthorized transaction within three working days, the customer has zero liability.
- The bank must restore the lost amount promptly.

**Judgment**

The Supreme Court upheld the Gauhati High Court ruling and held SBI fully liable for the fraudulent withdrawal. The bank was directed to refund the entire amount to the customer.

This judgment is considered landmark for several reasons:

1. Strengthening Consumer Protection: It reinforces the principle that customers should not suffer losses due to cyber fraud when they act diligently.[25]

[25] *State Bank of India v. Pallabh Bhowmick & Ors.*, Special Leave to Appeal (C) No. 30677/2024, 2025 INSC 12 (Supreme Court of India, Jan. 3, 2025

2. Accountability of Banks: Banks must maintain robust cybersecurity mechanisms and monitoring systems.

3. Recognition of Digital Banking Risks: The Court acknowledged the increasing risks associated with digital payments and emphasized institutional responsibility.

4. Precedent for Future Cyber-Fraud Cases: The ruling serves as an important precedent for disputes involving online banking fraud.

The case of *State Bank of India v. Pallabh Bhowmick* establishes a strong legal precedent emphasizing bank accountability in the era of digital banking. By reaffirming the RBI's zeroliability framework, the Supreme Court strengthened consumer protection and highlighted the responsibility of financial institutions to safeguard electronic transactions.

**Amazon Seller Services Pvt. Ltd. v. Unknown Persons / Amazonbuys.in (Delhi High Court)**

**Delhi High Court Ruling on Digital Fraud Infrastructure**

The case of Amazon Seller Services Pvt. Ltd. v. Amazonbuys.in & Ors. represents an important judicial response to digital fraud infrastructure and online trademark misuse. The Delhi High

Court addressed the misuse of Amazon's brand and platform through deceptive websites designed to defraud the public[26].

**Background of the Case**

Amazon Seller Services Pvt. Ltd., which operates the Amazon India online marketplace, discovered that certain websites and social-media accounts were fraudulently impersonating Amazon.

The defendants created websites such as Amazonbuys.in and related online pages that falsely represented themselves as official Amazon platforms. These platforms offered services such as:

- fake Amazon seller registrations
- franchise opportunities

[26] *Amazon Seller Services Pvt. Ltd. & Anr. v. Amazonbuys.in & Ors.*, CS (COMM) 364/2022, 2025:DHC:1104 (Delhi High Court, Feb. 27, 2025)

- online retail schemes

Unsuspecting users were induced to pay registration or participation fees.

**Legal Issues**

The key issues before the Delhi High Court were:

1. Whether the defendants' use of Amazon's name and logo constituted trademark infringement.
2. Whether the replication of Amazon's website design and content amounted to copyright infringement.
3. Whether the defendants were engaged in passing off and digital fraud.

Court's Observations

The Delhi High Court observed that the defendants deliberately copied the Amazon trademark, logos, and website interface to create confusion among consumers.

The Court noted that such fraudulent websites exploit the trust associated with well-known brands and cause financial loss to both consumers and the brand owner. The defendants' conduct amounted to:

- trademark infringement under the Trade Marks Act, 1999
- copyright infringement under the Copyright Act, 1957
- passing off and unfair competition.

The Court granted an ex-parte ad interim injunction, restraining the defendants from:

- using Amazon's trademark or logo
- operating deceptive websites resembling Amazon
- misleading consumers regarding affiliation with Amazon.

Additionally, the Court directed authorities such as internet service providers and government departments to block access to the fraudulent domains and online platforms.

This case is significant for several reasons:

1. Combating Digital Fraud Infrastructure It demonstrates how courts can disrupt online fraud networks through domain blocking and injunctions.
2. Protection of Well-Known Trademarks The judgment reinforces the legal

protection available to globally recognized brands.

3. Consumer Protection in E-Commerce The Court acknowledged the increasing risks faced by consumers in online marketplaces.

4. Judicial Approach to Online Impersonation The ruling illustrates how courts address anonymous or "unknown persons" operating fraudulent digital platforms.

The Delhi High Court's decision in *Amazon Seller Services Pvt. Ltd. v. Amazonbuys.in & Ors.* highlights the evolving challenges of digital fraud in the e-commerce sector. By granting injunctions and directing the blocking of fraudulent domains, the Court strengthened the legal framework for protecting both consumers and digital marketplaces from online impersonation and fraud.

**Challenges in the Existing Legal Framework**

Despite the presence of multiple regulatory laws governing digital payments, several challenges remain. One major issue is the lack of consumer awareness regarding digital security practices[27]. Many consumers remain unaware of the risks associated with sharing sensitive banking information online[28].

Another challenge relates to the jurisdictional complexities involved in investigating cybercrime, particularly when fraudulent activities originate from different geographical locations[29]. Additionally, the rapid pace of technological innovation often outpaces the development of legal regulations.

**Recommendations for Strengthening Consumer Protection**

To address the challenges associated with digital payment systems, several reforms may be considered.

First, stronger cybersecurity regulations should be implemented to ensure that financial institutions adopt advanced fraud detection systems. Second, regulatory authorities should establish clearer liability frameworks for fintech companies and digital payment intermediaries[30].

Third, public awareness campaigns should be conducted to educate consumers about safe

[27] Reserve Bank of India, Inauguration of Financial Literacy Week 2026
[28] Data Security Council of India (DSCI) & Seqrite, India Cyber Threat Report 2026 (Jan. 2026)
[29] Ministry of Home Affairs, Cybercrime in India 2025 Report, INSIGHTS IAS (Feb. 21, 2026).
[30] *Reserve Bank of India (Small Finance Banks - Digital Banking Channels Authorisation) Directions, 2025* (Effective Jan. 1, 2026).

digital payment practices. Finally, regulatory agencies should collaborate with law enforcement authorities to improve the investigation and prosecution of cyber fraud cases[31].

## Conclusion

Digital payment systems have become an integral component of India's modern financial infrastructure. These technologies offer numerous benefits, including convenience, efficiency, and financial inclusion. However, the increasing reliance on digital financial platforms has also created new legal challenges related to cybersecurity, consumer protection, and data privacy.

Although India has established several regulatory mechanisms to govern digital payments, gaps remain in the existing legal framework[32]. Strengthening consumer protection requires coordinated efforts involving regulatory authorities, financial institutions, technology providers, and consumers.

A balanced regulatory approach that encourages technological innovation while safeguarding consumer rights will play a crucial role in ensuring the sustainable growth of India's digital payment ecosystem[33].

[31] *Digital Personal Data Protection Rules, 2025* (G.S.R. notified Nov. 2025
[32] Reserve Bank of India, *Payments Vision 2025: Outcomes and 2030 Roadmap* (2026).
[33] Indian Cyber Crime Coordination Centre (I4C), *Annual Performance Report 2025*, Ministry of Home Affairs (2026).

## References


### I. Primary Legislation & Statutory Rules

1. Digital Personal Data Protection Rules, 2025, Notification No. G.S.R. 846(E) (Nov. 13, 2025).

2. The Payment and Settlement Systems Act, 2007 (Act No. 51 of 2007).

3. The Consumer Protection Act, 2019 (Act No. 35 of 2019) and the Consumer Protection (E-Commerce) Rules, 2020.

4. The Information Technology Act, 2000 (Act No. 21 of 2000).

### II. Landmark Judicial Precedents

1. *State Bank of India v. Pallabh Bhowmick & Ors.*, SLP (C) No. 30677/2024, 2025 INSC 12 (Supreme Court of India, Jan. 3, 2025).

2. *Amazon Seller Services Pvt. Ltd. & Anr. v. Amazonbuys.in & Ors.*, CS (COMM) 364/2022, 2025:DHC:1104 (Delhi High Court, Feb. 27, 2025).

3. *In Re: Digital-Arrest Scams*, Suo Motu Writ Petition (Crl.) No. 4/2025, 2026 INSC (Supreme Court of India, Feb. 9, 2026).

### III. Regulatory Directions & Frameworks (RBI)

1. Reserve Bank of India, *Authentication Mechanisms for Digital Payment Transactions Directions, 2025*, RBI/2025-26/1165 (Sept. 25, 2025).

2. Reserve Bank – Integrated Ombudsman Scheme (RB-IOS), 2026, Notification dated Jan.

16, 2026.

3. Reserve Bank of India, *Draft (Third Amendment) Directions: Responsible Business*

*Conduct – Customer Protection in Electronic Banking Transactions* (Mar. 6, 2026).

### IV. Official Reports & Metadata

1. Indian Cyber Crime Coordination Centre (I4C), *Annual Performance Review: Tackling Cyber-Enabled Frauds*, Ministry of Home Affairs (Feb. 2026).

2. Reserve Bank of India, *Payments Vision 2025: Final Achievement Report and Vision 2030 Roadmap* (Jan. 2026).