

Cybersecurity of Digital Payment Systems in India: Legal and Regulatory Challenges

Joylin Jacob Y¹, Parvathy Sb²

ABSTRACT

The rapid expansion of digital payment systems has fundamentally transformed the Indian financial ecosystem. Payment instruments such as Unified Payments Interface (UPI), mobile banking, internet banking, debit and credit cards, prepaid payment instruments, payment aggregators and digital wallets have facilitated faster, more convenient and increasingly accessible financial transactions. However, the growing dependence on digitally enabled payment infrastructure has simultaneously increased exposure to cybersecurity threats, including phishing, vishing, identity theft, SIM-swap fraud, malware attacks, credential theft, ransomware, social engineering, unauthorised electronic transactions and data breaches. The legal regulation of digital payment cybersecurity in India is therefore distributed across multiple statutes, regulatory directions and institutional mechanisms.

The Information Technology Act, 2000³, the Information Technology Rules, the Payment and Settlement Systems Act, 2007⁴, the Banking Regulation Act, 1949⁵, the Digital Personal Data Protection Act, 2023, and various directions issued by the Reserve Bank of India (RBI) collectively constitute the principal legal framework governing digital payment security. The RBI's 2021 Master Direction on Digital Payment Security Controls introduced common minimum-security standards for specified regulated entities, while the 2024 Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators further emphasise governance, data security, incident response, threat monitoring and resilience. Despite these developments, significant legal and regulatory challenges remain concerning allocation of liability for unauthorised transactions, third-party service-provider responsibility, cross-platform fraud, cybersecurity standards, data breaches, consumer awareness, digital evidence and coordination among regulatory and law-enforcement agencies. This paper critically examines India's existing legal and regulatory framework, analyses contemporary cybersecurity threats affecting digital payment systems, examines relevant judicial decisions and identifies gaps in the existing regime. It proposes a coordinated, risk-based and technologically adaptive regulatory framework to strengthen cybersecurity, consumer protection and institutional accountability in India's digital payment ecosystem.

Keywords: Cybersecurity, Digital Payments, UPI, Banking Law, Data Protection

1. INTRODUCTION AND BACKGROUND OF THE STUDY

India has undergone a substantial transformation from a predominantly cash-based economy towards a

¹ Author- JOYLIN JACOB Y* Research scholar in Bharath Institute of Higher Education and Research at school of law/ Assistant Professor in St. Joseph University, School of Law

² CO-AUTHOR: PARVATHY SD* Assistant Professor in St. Joseph University, School of Law

³ The Information Technology Act, 2000

⁴ The Payment and Settlement Systems Act, 2007

⁵ The Banking Regulation Act, 1949

digitally interconnected payment ecosystem. Technological advancement, widespread smartphone usage, internet connectivity, digital banking and government-supported financial inclusion initiatives have significantly increased the use of electronic payment mechanisms. Digital payment systems now constitute an important component of everyday economic activity, enabling individuals, businesses, financial institutions and government entities to transfer funds electronically. UPI, internet banking, mobile banking, payment cards, prepaid instruments, wallets and payment aggregators have consequently become important components of India's financial infrastructure.

The growth of digital payments has produced considerable benefits. Electronic transactions can reduce transaction time, facilitate financial inclusion, improve transparency and permit consumers to transfer money without physically visiting a bank branch. Digital payments have also contributed to the development of e-commerce and digital businesses. At the same time, the increasing dependence on interconnected information systems creates significant cybersecurity vulnerabilities. A payment transaction does not occur exclusively between a customer and a bank. It may involve banks, payment system operators, payment aggregators, telecom operators, technology service providers, application developers, cloud-service providers, merchants and other intermediaries. Consequently, a vulnerability at any point in the payment chain can potentially affect the security of the entire transaction.

Cybersecurity in digital payment systems involves more than preventing hacking. It encompasses confidentiality, integrity, availability, authentication, authorisation, non-repudiation, transaction monitoring, fraud detection, incident response and protection of personal and financial information. Attackers increasingly use social engineering techniques rather than merely exploiting technical vulnerabilities. Phishing messages, fraudulent customer-care calls, fake banking applications, malicious links, remote-access applications and SIM-swap techniques can persuade users to disclose or unknowingly compromise credentials. Indian courts have recognised phishing as an internet-fraud technique involving deceptive impersonation to obtain confidential information.

The legal response to these risks has developed incrementally. The Information Technology Act, 2000⁶ was India's principal legislation addressing electronic records, electronic authentication and cyber offences. Its provisions concerning unauthorised access, computer-related offences, identity theft, cheating by personation and privacy-related violations provide important criminal-law mechanisms. However, the Act predates the modern UPI, mobile-payment and platform-based payment ecosystem. Therefore, several aspects of contemporary digital-payment security are governed through sector-specific RBI directions rather than a single comprehensive cybersecurity statute.

The Payment and Settlement Systems Act, 2007⁷ provides an important statutory foundation for regulating payment systems. The RBI exercises significant regulatory authority over payment systems under this legislation. The framework is supplemented by RBI directions relating to payment systems, prepaid payment instruments, payment aggregators, customer protection and cybersecurity.

An important development was the RBI's Master Direction on Digital Payment Security Controls, 2021. The Direction sought to establish robust governance structures and common minimum-security standards for digital payment products and services. It applies to specified regulated entities including scheduled commercial banks, small finance banks, payments banks and credit-card issuing NBFCs.

⁶ The Information Technology Act, 2000

⁷ The Payment and Settlement Systems Act, 2007

The regulatory framework subsequently developed further with the RBI's Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, 2024. These Directions recognise the importance of cyber resilience and establish requirements relating to governance, risk assessment, data security, information-security management systems, vendor risk and payment security. They are issued under the Payment and Settlement Systems Act, 2007.

Another important component is the RBI's customer-protection regime for unauthorised electronic banking transactions. The 2017 framework introduced circumstances in which customers may have zero liability, particularly where the bank is responsible or where a third-party breach occurs without negligence by the bank or customer and the customer reports the transaction within the prescribed period. The framework also places the burden of proving customer liability on the bank.

Data protection represents another dimension of payment cybersecurity. Digital payment transactions generate extensive personal and financial information. Protection of such information is therefore connected with privacy and data-protection principles. The Digital Personal Data Protection Act, 2023⁸ provides a general statutory framework concerning processing and protection of digital personal data, although its implementation and interaction with sectoral financial regulation remain important areas for examination.

The contemporary digital-payment environment therefore presents a multidimensional legal problem. Cybersecurity must simultaneously address technological vulnerabilities, consumer protection, privacy, contractual responsibility, financial regulation, criminal liability and institutional accountability. A central question is whether India's existing fragmented legal framework is capable of providing adequate protection against increasingly sophisticated digital-payment fraud.

The issue is particularly significant because digital payment fraud can occur even when a consumer does not intentionally disclose credentials. Malware, SIM compromise, credential theft, compromised devices, fraudulent applications and sophisticated social-engineering techniques can blur the traditional distinction between "customer negligence" and "system failure". Courts are consequently required to examine whether liability should be imposed upon customers, banks, telecom operators, payment-system operators or other intermediaries.

Recent judicial developments illustrate this complexity. In *State Bank of India v. Hare Ram Singh* (2026)⁹, the Delhi High Court considered allegations involving unauthorised internet-banking transactions, phishing and OTP-based authentication and emphasised that questions concerning compromise of credentials, customer negligence and possible failure of security systems may require technical and forensic examination.

Thus, the cybersecurity of digital payment systems should not be viewed merely as a technological issue. It is fundamentally a legal and regulatory issue involving allocation of risk, protection of consumers, institutional responsibility, privacy, evidence and enforcement. This study examines these dimensions and seeks to identify legal and regulatory reforms necessary for creating a resilient and trustworthy digital payment environment in India.

2. OBJECTIVES OF THE STUDY

⁸ Personal Data Protection Act, 2023

⁹ In *State Bank of India v. Hare Ram Singh* (2026)

- To examine the existing legal and regulatory framework governing cybersecurity of digital payment systems in India.
- To analyse the major cybersecurity threats affecting UPI, internet banking, mobile banking, cards, wallets and other digital payment mechanisms.
- To examine judicial decisions concerning unauthorised electronic transactions, phishing, identity theft, SIM-swap fraud and banking cybersecurity.
- To identify gaps and inconsistencies in India's existing cybersecurity and digital-payment regulatory framework.
- To suggest legal and regulatory reforms for strengthening cybersecurity, consumer protection, institutional accountability and cyber-resilience in India's digital payment ecosystem.

3. RESEARCH GAP

Although considerable literature exists concerning cybercrime, banking fraud, data protection and digital payments, a significant research gap remains at the intersection of these areas.

First, existing studies frequently examine cybersecurity as a technological problem while giving comparatively limited attention to the allocation of legal responsibility among banks, payment-system operators, payment aggregators, telecom operators, technology vendors and customers

Second, the legal framework remains distributed across several statutes and RBI directions. There is no single comprehensive legislative framework specifically dealing with cybersecurity of the entire digital-payment ecosystem.

Third, existing research often focuses on conventional unauthorised banking transactions. Contemporary fraud increasingly involves social engineering, SIM swapping, malicious applications, remote-access tools, deepfake-enabled impersonation, account takeover and coordinated attacks across multiple service providers.

Fourth, the distinction between customer negligence and system-level cybersecurity failure is becoming increasingly difficult to establish. The RBI framework provides important protections, but judicial decisions demonstrate that disputes may require detailed technical and forensic examination.

Fifth, there remains a need to examine the relationship between the RBI's cybersecurity framework and India's evolving data-protection regime.

The present study seeks to fill this gap by providing an integrated legal analysis of cybersecurity, consumer liability, institutional responsibility, data protection and regulatory governance within India's digital-payment ecosystem.

4. EXISTING LEGAL AND REGULATORY FRAMEWORK

4.1 INFORMATION TECHNOLOGY ACT, 2000¹⁰

The Information Technology Act, 2000 is one of the principal statutory foundations of India's cyber-law regime. Several provisions are relevant to digital payment security

Section 43 addresses unauthorised access, downloading or extraction of data, introduction of viruses and damage to computer systems. Section 43A historically provided compensation for failure by a body corporate to implement reasonable security practices in relation to sensitive personal data or information.

¹⁰ Ibid

Section 65 deals with tampering with computer source documents, while Section 66 criminalises computer-related offences involving dishonest or fraudulent acts contemplated by Section 43.

Section 66C addresses identity theft and is particularly relevant to digital payment fraud involving passwords, electronic signatures and other unique identification features. Section 66D addresses cheating by personation using a computer resource or communication device. These provisions may apply to several forms of online banking and payment fraud. The statutory framework expressly treats identity theft as a cyber offence.

Section 72 addresses breach of confidentiality and privacy in specified circumstances. Section 72A addresses disclosure of information in breach of lawful contract.

However, the IT Act has limitations. Many provisions were drafted when India's digital environment was substantially different from today's UPI and mobile-payment ecosystem. The Act therefore operates alongside sector-specific regulatory directions rather than constituting a complete digital-payment cybersecurity code.

4.2 PAYMENT AND SETTLEMENT SYSTEMS ACT, 2007¹¹

The Payment and Settlement Systems Act, 2007 provides the statutory foundation for regulation and supervision of payment systems in India.

The Act empowers the RBI to regulate and supervise payment systems. The RBI's cybersecurity directions for payment-system operators derive authority from the Act. The 2024 Master Directions for non-bank Payment System Operators expressly rely upon Sections 10(2) and 18 of the PSS Act.

The importance of the Act lies in its institutional approach. Rather than treating payment fraud solely as an individual cybercrime, it recognises payment systems as regulated financial infrastructure requiring systemic oversight.

4.3 RBI MASTER DIRECTION ON DIGITAL PAYMENT SECURITY CONTROLS, 2021¹²

The 2021 Master Direction represents one of the most significant developments in India's digital-payment cybersecurity framework. It establishes common minimum-security standards for specified regulated entities. Its coverage includes scheduled commercial banks excluding RRBs, small finance banks, payments banks and credit-card issuing NBFCs. The framework requires security governance, application-security controls, encryption, monitoring and incident-management mechanisms. Digital payment applications are expected to follow a secure-by-design approach.

The Direction also requires regulated entities to undertake security testing, including vulnerability assessment and penetration testing. Application security is therefore treated as an ongoing lifecycle responsibility rather than a one-time compliance exercise. It also addresses web application firewalls, DDoS mitigation, strong cryptographic standards, logging, monitoring and multi-tier application architecture.

4.4 RBI MASTER DIRECTIONS ON CYBER RESILIENCE AND DIGITAL PAYMENT SECURITY CONTROLS, 2024¹³

The 2024 Master Directions significantly strengthen the regulatory framework applicable to authorised non-bank Payment System Operators.

The Directions focus upon:

- cyber-risk governance;

¹¹ Ibid

¹² RBI MASTER DIRECTION ON DIGITAL PAYMENT SECURITY CONTROLS, 2021

¹³ RBI MASTER DIRECTIONS ON CYBER RESILIENCE AND DIGITAL PAYMENT SECURITY CONTROLS, 2024

- identification and assessment of cyber risks;
- cyber-resilience;
- data security;
- information-security management systems;
- vendor risk;
- incident response;
- threat monitoring;
- anti-phishing measures;
- transaction monitoring;
- customer awareness;
- security of payment architecture.

The Directions require protection of business and customer information both at rest and in transit and require appropriate encryption and information-security mechanisms. They also require PSOs to implement mechanisms for detecting unusual transaction behaviour based on parameters including transaction velocity, IP address, geolocation, behavioural biometrics and other indicators. This is an important transition from traditional cybersecurity compliance towards risk-based cyber resilience.

4.5 RBI CUSTOMER PROTECTION FRAMEWORK, 2017¹⁴

The RBI's 2017 framework concerning unauthorised electronic banking transactions is particularly significant from the consumer-protection perspective. The framework recognises zero liability where: there is contributory fraud, negligence or deficiency by the bank; or a third-party breach occurs where neither the bank nor customer is responsible and the customer reports the transaction within three working days.

Where the customer is negligent, such as by sharing payment credentials, the customer bears the loss until reporting the transaction. Loss occurring after reporting is borne by the bank. Importantly, the RBI framework places the burden of proving customer liability on the bank. This provision is particularly significant because it prevents the mere occurrence of an unauthorised transaction from automatically establishing customer negligence.

4.6 PREPAID PAYMENT INSTRUMENTS

RBI's regulatory framework for prepaid payment instruments also contains cybersecurity and customer-protection mechanisms. PPI issuers are required to establish mechanisms for monitoring and handling cybersecurity incidents and breaches. The framework also incorporates customer-protection mechanisms concerning unauthorised transactions. The PPI framework is particularly relevant to wallets and other stored-value digital payment instruments.

4.7 DIGITAL PERSONAL DATA PROTECTION ACT, 2023¹⁵

Digital payment systems process large volumes of personal information, including names, mobile numbers, account information, transaction details and identification information. The Digital Personal Data Protection Act, 2023 introduces a general statutory framework concerning digital personal data. For payment institutions, data governance must therefore be considered alongside financial-sector cybersecurity requirements.

¹⁴ 4.5 RBI CUSTOMER PROTECTION FRAMEWORK, 2017

¹⁵ Ibid

A significant regulatory challenge is ensuring consistency between general data-protection obligations and sector-specific RBI cybersecurity requirements. Payment institutions may simultaneously be subject to obligations arising from financial regulation, cybersecurity directions, contractual arrangements and data-protection law.

4.8 CERT-IN DIRECTIONS

The Indian Computer Emergency Response Team (CERT-In) plays an important role in national cybersecurity incident response. The regulatory framework concerning incident reporting, log retention and cybersecurity incident management becomes particularly relevant to financial institutions and payment intermediaries.

Effective cooperation between RBI-regulated entities and CERT-In is important because digital payment incidents can rapidly become systemic rather than remaining isolated customer disputes.

4.9 CONSUMER PROTECTION FRAMEWORK

Digital payment users may also invoke consumer-protection mechanisms where a banking or payment service involves deficiency in service. However, consumer proceedings can become complicated when the dispute involves highly contested facts concerning cybercrime, fraud, authentication or technical compromise. Courts have recognised that complicated allegations of fraud may require detailed adjudication rather than summary consumer proceedings.

4.10 INDIAN CONTRACT ACT, 1872¹⁶

Contractual relationships remain important in digital payment transactions. Banks and payment intermediaries establish terms concerning authentication, security credentials, liability and customer obligations. However, contractual terms cannot necessarily override mandatory regulatory protections. RBI directions concerning customer liability operate as an important regulatory framework for determining responsibility for unauthorised transactions.

5. CONTEMPORARY CYBERSECURITY ISSUES

5.1 PHISHING AND VISHING

Phishing remains one of the most significant threats. Fraudsters impersonate banks, payment companies, government agencies or trusted persons to obtain credentials. Vishing uses telephone communication, while smishing uses fraudulent SMS messages. The Delhi High Court recognised phishing as an internet-fraud method involving impersonation to obtain confidential information.

5.2 SIM-SWAP FRAUD

SIM-swap fraud exploits the relationship between telecommunications services and OTP-based banking authentication. A fraudster obtains a replacement SIM and receives OTPs intended for the legitimate customer. This demonstrates that digital-payment cybersecurity cannot be addressed exclusively by banks. In *Tony Enterprises v. RBI*, the Kerala High Court examined SIM-swap fraud and described it as a form of identity theft in cyberspace, connecting such conduct with Section 66C of the IT Act.

5.3 OTP-BASED AUTHENTICATION

OTP authentication is widely used as an additional security mechanism. However, OTPs do not provide absolute security where the underlying mobile device, SIM, credentials or communication channel is compromised.

¹⁶ INDIAN CONTRACT ACT, 1872

The 2026 SBI v. Hare Ram Singh litigation illustrates the legal difficulty in determining whether an OTP-based transaction resulted from customer negligence or compromise of the security system.

5.4 MALWARE AND REMOTE-ACCESS APPLICATIONS

Fraudsters increasingly persuade victims to install remote-access or malicious applications. Such applications may allow criminals to observe screens, intercept information or manipulate transactions. The legal challenge is determining whether the victim's installation of the application constitutes "customer negligence" or whether the payment institution failed to implement adequate fraud-detection mechanisms.

5.5 ACCOUNT TAKEOVER

Account takeover occurs when an attacker gains control of a customer's digital banking account. This can occur through stolen credentials, SIM compromise, malware, phishing or leaked personal information. Because modern payment accounts may be connected to multiple services, account takeover can facilitate rapid transfers across multiple institutions.

5.6 DATA BREACHES

Payment institutions hold highly valuable personal and financial data. A cybersecurity breach may therefore produce consequences extending beyond one fraudulent transaction. Data breaches raise questions concerning notification, accountability, compensation, data minimisation, security safeguards and regulatory oversight.

5.7 PAYMENT AGGREGATOR AND VENDOR RISK

Digital payment systems frequently depend upon third-party technology providers. A bank or payment operator may outsource infrastructure, cloud services, application development, security monitoring or other functions. Consequently, cybersecurity responsibility cannot be limited to the regulated entity alone. The 2024 RBI framework addresses this problem by incorporating vendor-risk management and requiring assurance concerning cyber resilience for vendors involved in critical processes.

5.8 CROSS-PLATFORM FRAUD

A single fraudulent transaction may involve a telecom operator, bank, UPI application, payment aggregator and beneficiary bank. This creates jurisdictional and institutional complexity. A coordinated legal framework is therefore necessary to determine responsibility and facilitate rapid freezing and recovery of fraudulent funds.

5.9 DEEPFAKES AND AI-ENABLED FRAUD

Artificial intelligence creates new possibilities for financial fraud. Voice cloning, synthetic identities, manipulated videos and AI-generated communications can make impersonation substantially more convincing. Existing laws can potentially apply to such conduct, but the evidentiary and attribution challenges associated with AI-generated fraud require further legal development.

5.10 CUSTOMER AWARENESS

Cybersecurity is partly dependent upon user behaviour. RBI regulations already recognise customer awareness as an important security measure. The 2024 framework requires payment-system operators to create public awareness concerning payment fraud and cyber threats.

However, awareness campaigns must evolve continuously because fraudulent techniques change rapidly.

6. CASE LAWS

1. NATIONAL ASSOCIATION OF SOFTWARE AND SERVICE COMPANIES V. AJAY SOOD & OTHERS, 2005¹⁷

Facts: Fraudsters created deceptive e-mail identities and attempted to obtain confidential information by impersonating legitimate organisations. The case became one of India's early judicial discussions of phishing.

Judgment: The Delhi High Court recognised phishing as a form of internet fraud involving misrepresentation and extraction of confidential information. The Court discussed the absence of specific Indian legislation expressly dealing with phishing at that time.

Relevance: The case demonstrates the early judicial recognition of phishing and the need for cyber-specific legal responses.

2. TONY ENTERPRISES V. RESERVE BANK OF INDIA, 2019¹⁸

Facts: The case concerned SIM-swap fraud and the resulting risks associated with unauthorised electronic banking transactions.

Judgment: The Kerala High Court examined SIM swapping as a form of identity theft in cyberspace and referred to Section 66C of the Information Technology Act.

Relevance: The decision demonstrates that digital-payment security is connected with telecommunications security and identity protection.

3. ICICI BANK LTD. V. UMA SHANKAR SIVASUBRAMANIAN

Facts: The case involved allegations concerning phishing and disclosure of banking information through fraudulent electronic communications.

Judgment: The judicial discussion considered the circumstances in which a customer may have disclosed information in response to phishing communications and the bank's responsibilities concerning customer security.

Relevance: The case demonstrates the difficulty in distinguishing customer negligence from deficiencies in banking security.

4. TONY ENTERPRISES V. RBI – CUSTOMER LIABILITY ISSUE¹⁹

Facts: The dispute involved unauthorised electronic transactions and the application of RBI's customer-protection framework.

Judgment: The Kerala High Court examined the RBI framework concerning zero liability and limited liability for unauthorised transactions.

Relevance: The decision demonstrates the importance of RBI directions in determining liability for digital-payment fraud.

5. HARE RAM SINGH V. RESERVE BANK OF INDIA & OTHERS, 2024²⁰

Facts: The petitioner challenged the handling of unauthorised electronic transactions and relied upon RBI's customer-protection framework.

Judgment: The Delhi High Court discussed the RBI circular and its provisions concerning zero liability, third-party breach and customer negligence.

¹⁷ NATIONAL ASSOCIATION OF SOFTWARE AND SERVICE COMPANIES V. AJAY SOOD & OTHERS, 2005

¹⁸ Tony Enterprises V. Reserve Bank Of India, 2019

¹⁹ Tony Enterprises V. Rbi – Customer Liability Issue

²⁰ . Hare Ram Singh V. Reserve Bank Of India & Others, 2024

Relevance: The decision illustrates the importance of timely reporting and the legal framework for determining customer liability.

6. STATE BANK OF INDIA V. HARE RAM SINGH, 2026²¹

Facts: Unauthorised internet-banking transactions resulted in substantial financial loss. The dispute concerned OTP authentication, phishing and whether the customer had compromised his credentials.

Judgment: The Delhi High Court's 2026 judgment emphasised that questions concerning compromise of user credentials, OTPs, malware and security-system failure can involve technical and forensic issues. It examined the relationship between the RBI's 2017 customer-liability framework and the 2021 Digital Payment Security Controls.

Relevance: The case is highly relevant to the present research because it demonstrates the modern judicial problem of attributing responsibility in sophisticated digital-payment fraud.

7. NAYNA BIPIN VORA V. BANK OF BARODA, 2026²²

Facts: Fraudulent transactions resulted in approximately ₹18.79 lakh being transferred from the petitioners' account. The petitioners alleged that the transactions occurred because of third-party cyber fraud.

Judgment: The Bombay High Court held that the RBI's 2017 customer-protection framework operates independently of criminal investigation. The Court held that the burden of proving customer liability rested upon the bank and directed reversal of the amount with interest where the bank failed to establish customer fault.

Relevance: The judgment strongly illustrates the consumer-protection dimension of RBI's digital-payment framework.

8. PNP POLYTEX PRIVATE LIMITED V. RESERVE BANK OF INDIA, 2026²³

Facts: The case concerned unauthorised electronic banking transactions and the application of RBI's customer-protection framework.

Judgment: The Bombay High Court discussed the RBI's zero-liability mechanism and reiterated the importance of determining whether the customer was responsible for the unauthorised transaction.

Relevance: The case demonstrates continuing judicial interpretation of the RBI framework.

9. BASAVESHWARA PATTANA SAHAKARA BANK NIYAMITHA V. BSNL, 2026²⁴

Facts: Cyber fraudsters allegedly obtained a duplicate SIM from BSNL and used it to gain access to net-banking facilities. The incident resulted in financial loss to a cooperative bank.

Judgment: The Karnataka High Court held BSNL liable for negligence and deficiency and directed payment of compensation of ₹55 lakh. The judgment highlighted the importance of the integrity of OTP-based authentication systems.

Relevance: This case demonstrates that cybersecurity responsibility may extend beyond banks to telecommunications operators.

10. ANEESH KHAN V. STATE BANK OF INDIA, 2026²⁵

Facts: The complainant alleged unauthorised transactions following disclosure of card-related information to an unknown caller.

²¹ State Bank Of India V. Hare Ram Singh, 2026

²² Nayna Bipin Vora V. Bank Of Baroda, 2026

²³ Pnp Polytex Private Limited V. Reserve Bank Of India, 2026

²⁴ Basaveshwara Pattana Sahakara Bank Niyamitha V. Bsnl, 2026

²⁵ Aneesh Khan V. State Bank Of India, 2026

Judgment: The consumer forum considered the RBI framework and observed that where loss results from customer negligence, the customer may bear the loss until reporting the transaction. The case also recognised the limitations of summary consumer proceedings when allegations involve complex fraud and criminality.

Relevance: The decision demonstrates the interaction between customer negligence, RBI directions and consumer jurisdiction.

7. RESEARCH GAP: ANALYTICAL FINDINGS

The examination of legislation, regulatory directions and judicial decisions demonstrates that India's cybersecurity framework is extensive but fragmented.

The first gap concerns uniformity of cybersecurity standards. Different participants in the payment ecosystem may be subject to different regulatory requirements. Although the RBI has significantly strengthened its framework, the complete payment chain may involve entities regulated under different legal regimes.

The second gap concerns third-party liability. Payment transactions increasingly involve intermediaries and technology vendors. Determining responsibility where the vulnerability occurs at a vendor, telecom operator or intermediary remains legally complex.

The third gap concerns customer negligence. Traditional approaches may treat disclosure of credentials as decisive evidence of customer responsibility. However, sophisticated malware, SIM compromise and social engineering can produce unauthorised transactions without deliberate disclosure.

The fourth gap concerns cross-platform coordination. Fraud may involve multiple banks, payment platforms, telecom operators and jurisdictions.

The fifth gap concerns rapid technological change. Legal rules may become outdated when technologies such as artificial intelligence, biometric authentication and tokenisation develop faster than legislation.

The sixth gap concerns digital evidence. Cybersecurity disputes frequently depend upon transaction logs, IP addresses, device fingerprints, authentication records and forensic evidence. Uniform evidentiary standards and preservation procedures are therefore essential.

8. SUGGESTIONS AND RECOMMENDATIONS

8.1 ENACT A COMPREHENSIVE DIGITAL PAYMENT CYBERSECURITY FRAMEWORK

India should consider developing a consolidated legislative framework dealing specifically with cybersecurity of digital payment infrastructure. Such a framework need not replace the IT Act, PSS Act or RBI directions but could harmonise them.

8.2 ESTABLISH UNIFORM LIABILITY PRINCIPLES

A statutory framework should clearly distinguish:

- customer negligence;
- bank negligence;
- payment-system failure;
- telecom failure;
- third-party vendor failure;
- systemic cyberattack; and
- unavoidable external breach.
- This would reduce inconsistent treatment of victims.

8.3 STRENGTHEN REAL-TIME FRAUD DETECTION

Banks and payment operators should increasingly use behavioural analytics, transaction velocity, device intelligence, geolocation and anomaly detection.

The RBI's 2024 framework already recognises several such indicators.

8.4 STRENGTHEN TELECOM-BANKING COORDINATION

SIM-swap fraud demonstrates that banking cybersecurity cannot operate independently from telecommunications security. SIM replacement involving financial accounts should therefore be accompanied by enhanced risk controls.

8.5 CREATE A CENTRALISED DIGITAL PAYMENT FRAUD RESPONSE MECHANISM

A coordinated mechanism involving banks, payment-system operators, telecom companies, RBI, CERT-In and law-enforcement authorities should facilitate rapid freezing and tracing of fraudulent transactions.

8.6 STRENGTHEN VENDOR ACCOUNTABILITY

Critical technology vendors should be subjected to mandatory cybersecurity audits, contractual security obligations, incident-reporting requirements and liability provisions.

8.7 IMPROVE CUSTOMER AWARENESS

Awareness should move beyond generic warnings such as "do not share OTP".

Consumers should be educated about:

- fake customer-care numbers;
- screen-sharing applications;
- malicious QR codes;
- SIM-swap fraud;
- fraudulent UPI collect requests;
- fake KYC messages;
- deepfake communications;
- investment scams; and
- remote-access applications.

8.8 DEVELOP SPECIALISED CYBER COURTS OR BENCHES

Complex digital-payment disputes frequently require technical expertise. Specialised judicial mechanisms could improve consistency and reduce delays.

8.9 STRENGTHEN DIGITAL EVIDENCE STANDARDS

Banks and payment providers should preserve relevant logs, device information, IP records, authentication data and transaction metadata for appropriate periods.

8.10 INTRODUCE RISK-BASED AUTHENTICATION

Authentication should not rely exclusively upon OTPs. High-risk transactions should trigger additional authentication based on behavioural, device or biometric indicators.

9. CONCLUSION

The rapid expansion of digital payment systems has transformed India's financial ecosystem while simultaneously creating a complex cybersecurity environment. Digital payments provide substantial economic and social benefits, but their security depends upon the coordinated functioning of banks, payment-system operators, technology providers, telecom companies, customers and regulatory authorities.

India has developed a substantial regulatory framework through the Information Technology Act, 2000, Payment and Settlement Systems Act, 2007, RBI directions, customer-protection mechanisms, cybersecurity regulations and the Digital Personal Data Protection Act, 2023. The RBI's 2021 Digital Payment Security Controls and 2024 Cyber Resilience Directions demonstrate a clear movement towards stronger governance, secure-by-design principles, data protection, threat monitoring and cyber resilience. Nevertheless, technological developments have created challenges that cannot be addressed exclusively through traditional legal concepts. Phishing, SIM swapping, malware, account takeover, AI-enabled impersonation and third-party vulnerabilities demonstrate that responsibility may extend across several participants.

The principal requirement is therefore an integrated legal and regulatory approach. Cybersecurity obligations should be clearly allocated, customer protection should remain central, payment intermediaries should be accountable, and regulatory institutions should be capable of responding rapidly to emerging threats. India's future digital-payment ecosystem will depend not merely upon increasing transaction volumes but upon maintaining public confidence in the security, reliability and legal accountability of digital financial infrastructure.

11. REFERENCES

STATUTES

1. Information Technology Act, 2000.
2. Payment and Settlement Systems Act, 2007.
3. Banking Regulation Act, 1949.
4. Reserve Bank of India Act, 1934.
5. Digital Personal Data Protection Act, 2023.
6. Consumer Protection Act, 2019.
7. Indian Contract Act, 1872.
8. Bharatiya Nyaya Sanhita, 2023.
9. Bharatiya Sakshya Adhiniyam, 2023.
10. RBI Materials
11. RBI, Master Direction on Digital Payment Security Controls, 2021. The Direction establishes common minimum-security standards for specified regulated entities.
12. RBI, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, 2017.
13. RBI, Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, 2024.
14. RBI, Master Directions on Prepaid Payment Instruments.
15. RBI, directions concerning Online Dispute Resolution for digital payments.

IMPORTANT JUDICIAL SOURCES

1. National Association of Software and Service Companies v. Ajay Sood & Others, Delhi High Court, 2005.
2. Tony Enterprises v. Reserve Bank of India, Kerala High Court, 2019.
3. Hare Ram Singh v. Reserve Bank of India & Others, Delhi High Court, 2024.
4. State Bank of India v. Hare Ram Singh, Delhi High Court, 2026.
5. Nayna Bipin Vora v. Bank of Baroda, Bombay High Court, 2026.

6. PNP Polytex Private Limited v. Reserve Bank of India, Bombay High Court, 2026.
7. Basaveshwara Pattana Sahakara Bank Niyamitha v. BSNL, Karnataka High Court, 2026.
8. Aneesh Khan v. State Bank of India, State Consumer Disputes Redressal Commission, 2026.
9. Chairman & Managing Director, City Union Bank Ltd. v. R. Chandramohan, Supreme Court, 2023 — relevant to the limits of summary consumer proceedings where complex fraud/criminality is involved.